ADPRO®
XOa Client Software

User Manual

For FastTrace 2 Series

March 16, 2015
Doc. 21796_05_preliminary
Version XOa 3.00.0005

ADPRO® by xtralis®

Disclaimer

The contents of this document are provided on an "as is" basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.

Intellectual Property and Copyright

This document includes registered and unregistered trademarks. All trademarks displayed are the trademarks of their respective owners. Your use of this document does not constitute or create a license or any other right to use the name and/or trademark and/or label. This document is subject to copyright owned by Xtralis. You agree not to copy, communicate to the public, adapt, distribute, transfer, sell, modify, or publish any contents of this document without the express prior written consent of Xtralis.

General Warning

This product must only be installed, configured and used strictly in accordance with the General Terms and Conditions, User Manual and product documents available from Xtralis. All proper health and safety precautions must be taken during the installation, commissioning, and maintenance of the product. The system should not be connected to a power source until all the components have been installed. Proper safety precautions must be taken during tests and maintenance of the products when these are still connected to the power source. Failure to do so or tampering with the electronics inside the products can result in an electric shock causing injury or death and may cause equipment damage. Xtralis is not responsible and cannot be held accountable for any liability that may arise due to improper use of the equipment and/or failure to take proper precautions. Only persons trained through an Xtralis accredited training course can install, test and maintain the system.

Liability

You agree to install, configure, and use the products strictly in accordance with the User Manual and product documents available from Xtralis.

Xtralis is not liable to you or any other person for incidental, indirect, or consequential loss, expense or damages of any kind including without limitation, loss of business, loss of profits, or loss of data arising out of your use of the products. Without limiting this general disclaimer the following specific warnings and disclaimers also apply:

Fitness for Purpose

You agree that you have been provided with a reasonable opportunity to appraise the products and have made your own independent assessment of the fitness or suitability of the products for your purpose. You acknowledge that you have not relied on any oral or written information, representation, or advice given by or on behalf of Xtralis or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Xtralis in relation to the products is limited to:
(i) in the case of services, the cost of having the services supplied again; or
(ii) in the case of goods, the lowest cost of replacing the goods, acquiring equivalent goods or having the goods repaired.

Indemnification

You agree to fully indemnify and hold Xtralis harmless for any claim, cost, demand, or damage (including legal costs on a full indemnity basis) incurred or which may be incurred arising from your use of the products.

Miscellaneous

If any provision outlined above is found to be invalid or unenforceable by a court of law, such invalidity or unenforceability will not affect the remainder which will continue in full force and effect. All rights not expressly granted are reserved.

Document Conventions

The following typographic conventions are used in this document.

Convention	Description
Bold	Used to denote: emphasis. Used for names of menus, menu options, toolbar buttons.
Italics	Used to denote: references to other parts of this document or other documents. Used for the result of an action.

The following icons are used in this document.

Icon	Description
	Note. This icon indicates information of special interest that will help the reader make full use of the product, optimise performance, etc. Failure to read the note will not result in physical harm to the reader, or damage to equipment or data.
	Caution! This icon indicates danger to equipment. The danger can be loss of data, physical damage to the equipment, or permanent corruption of configuration details.
	Warning! This icon indicates danger of physical harm to the reader. Not following instructions may lead to death or permanent injury.
	Warning! This icon indicates danger of electric shock. This may lead to death or permanent injury.
	Warning! This icon indicates that there is a danger of inhaling dangerous substances. This may lead to death or permanent injury.

Trade Name Statement

ADPRO is a registered trademark of Xtralis Pty Ltd.

Contact Us

UK and Europe +44 1442 242 330 **D-A-CH** +49 431 23284 1 **The Americas** +1 781 740 2223
Middle East +962 6 588 5622 **Asia** +86 21 5240 0077 **Australia and New Zealand** +61 3 9936 7000
www.xtralis.com

Contents

1 About this Manual 10

1.1 What is XOa 3? 10

1.2 Scope 10

2 Installing the XOa Client Software 11

2.1 System Requirements 11

2.1.1 Hardware 11

2.1.2 Software 11

2.2 Preparing Your PC for Installation 11

2.2.1 Internet Explorer Settings 11

2.2.2 Changing the PC's IP Address 13

2.3 Installing the XOa Client Software 16

2.4 Launching and Initial Configuration 19

2.4.1 Launching the XOa Client in Internet Explorer 19

2.4.2 Launching the XOa Client in Its Own Window 20

2.4.3 Adding a Server to the XOa Client 21

2.4.4 Changing a Server 23

2.4.5 Setting Date and Time 23

3 Connections 25

3.1 Network and Modem (Ethernet/PPP) 25

3.1.1 Ports 25

3.1.2 Ethernet Connection 26

3.1.3 Granting Access to the Server 28

3.1.4 PPP Connection 28

3.2 IP Camera Network Configuration 32

3.2.1 General Setup 32

3.2.2 Ethernet Cards 33

3.2.3 HIPI Cards 33

3.3 Audio 35

3.3.1 Audio IN 35

3.3.2 Audio OUT 35

3.4 Internal I/O Cards 36

3.4.1 Updating the Main I/O card 38

3.4.2 USB I/O Address Range 38

3.5 Net I/O Modules 39

3.5.1 Ordering Information 41

3.5.2 Net I/O Address Range 41

3.5.3 Adding Net I/O Module with Known IP Address 42

3.5.4 Searching Net I/O Modules on the Local Network 43

3.5.5 Modifying the IP Settings of a Net I/O Module 43

3.5.6 Net I/O Module Inputs and Outputs Setup 43

3.6 Connection to Presidium 44

3.7 Connection to S3100 45

3.8 Email 47

3.8.1 Setting up Email 47

3.8.2 Creating Mailing Lists 48

3.8.3 Verifying Email Communication 50

4 Using IP Cameras 51

4.1 RMG Units with HIPI Card (FastTrace 2 Series Only) 51

4.2 RMG Units with IP Gateway Card (FastTrace 2 Series Only) 51

4.3 IP Camera Setup 51
4.3.1 General Parameters 53
4.3.2 Video Settings 54
4.3.3 Brightness/Contrast/Saturation 54
4.3.4 Overlay 54
4.3.5 Network 54
4.3.6 PTZ 55
4.3.7 Recording 55

5 Using Analogue Cameras 57
5.1 Video and Audio Connections 57
5.2 Analogue Camera Setup 57
5.2.1 General Parameters 58
5.2.2 Video Settings 58
5.2.3 Brightness/Contrast/Saturation 58
5.2.4 Overlay 58
5.2.5 Network 59
5.2.6 PTZ 59
5.2.7 Recording 60
5.3 List of Available PTZ Protocols 60
5.4 PTZ Control via USB Port/MIO Card 61
5.5 PTZ Control via DTC Card 62

6 Recording Mode Schedule 63
6.1 Operational Modes 63
6.2 Operational Mode with Time Schedule 63
6.3 Operational Mode with Manual Selection 64

7 Recordings Behaviour 66
7.1 Setting up Recordings 66
7.1.1 Name 67
7.1.2 Cameras 67
7.2 Continuous Recording 67
7.3 Recording on Event 68

8 Watching Live Images 71
8.1 Watching Live Images in the Live Video Screen 71
8.1.1 Live Video Streaming Limitations 73
8.1.2 Tools 74
8.1.3 Audio 77
8.1.4 PTZ Control 78
8.2 Watching Live Images on a Monitor 79
8.2.1 About Using a Monitor 79
8.2.2 Setting up a Monitor 79
8.2.3 Disabling the Matrix View 80
8.2.4 Switching Between Matrix View and Welcome Screen 80

9 Searching Recordings and Watching Events 82
9.1 Searching Recordings on the Timeline 82
9.1.1 Types of Video Recordings 82
9.1.2 Searching on the Timeline 83
9.1.3 Searching Recordings of Events 83
9.1.4 Playing the Selected Video Footage 84
9.1.5 Synchronised Playback 84
9.2 Searching Recordings via Advanced Search 86

9.3 Searching Recordings via Postmotion 88
9.4 Downloading and Storing Selected Video Recordings 89
9.5 Locked Recordings 90
9.6 Managing Local Recordings 91
9.7 Automatically Erasing Old(er) Video Recordings 92

10 360° Camera Images 94

11 Arm/Disarm Schedule 95

12 Alarm Profiles 97
12.1 About Alarm Profiles 97
12.2 Adding a New Profile 97
12.3 Deleting an Alarm Profile 99
12.4 Default Profiles 99
12.4.1 Normal Event Profile 100
12.4.2 Primary Event Profile 100
12.4.3 Backup Event Profile 101
12.4.4 Silent Message Profile 102
12.4.5 Single Event Profile 102
12.4.6 Active Sensor Event Profile 103
12.4.7 Fire Primary Profile 104
12.4.8 Fire Advisory Profile 105
12.4.9 Fire Verification Profile 105
12.4.10 Fire Trouble Profile 106

13 Input/Output Behaviour 107
13.1 Alarm Input Behaviour 107
13.2 PTZ via I/O 109
13.3 Connecting Fire Detectors 109
13.3.1 Fire Reset Input and Output (SmokeTrace Stop Input) 110
13.4 IntrusionTrace Alarms 111
13.5 PIR Alarms 112
13.6 Arm/Disarm Switch 114
13.7 Activating Outputs 115
13.7.1 Manual Operation 116
13.7.2 Recording Controlled 116
13.7.3 Programmable Output 116

14 Alarm Transmission 118
14.1 General 118
14.2 Primary Alarm Transmission Settings 119
14.3 Secondary Alarm Transmission Settings 120
14.4 Setting up Parallel Transmission 121

15 Analytics 123
15.1 The Xtralis Xapps 123
15.2 Motion, Sabotage 123
15.2.1 Motion, Sabotage Interface 123
15.2.2 Cameras 123
15.2.3 Drawing Tools 124
15.2.4 Motion Detection Zones 124
15.2.5 Private Zones 125
15.2.6 Motion Zone Detection Settings 126

15.2.7 Sabotage Detection 127

16 PIR Settings 128

16.1 Required PIR Firmware 128
16.2 Connecting the PIRs 128
16.3 Configuring the Software Settings 128
16.3.1 Configuring the Serial Port 128
16.3.2 Initiating the PIR Discovery 129
16.4 Double-Knock Configuration 130

17 Calendar 133

18 Users 134

18.1 About Users 134
18.2 About Strong Passwords 134
18.3 Adding New Users 134
18.4 User Rights 135
18.4.1 Live Video 136
18.4.2 Recorded Video 137
18.4.3 System 138
18.4.4 Status 138
18.4.5 General 139
18.5 Modifying or Deleting an Existing User 139
18.6 Granting the Technician 140

19 Uploading and Downloading Files 141

19.1 Uploading Files to the Server 141
19.2 Downloading Files from the Server 142

20 Configuration Management 143

20.1 Storing a Configuration 143
20.2 Copying Configurations 143
20.3 Activating a Configuration 144

21 Factory Defaults 145

22 Starting and Stopping 146

23 Status 147

23.1 Status Indicators 147
23.2 Isolating an Alarm Input 149
23.3 Activating an Output Manually 149
23.4 General Status of the Video System 149

24 System Information 151

24.1 Checking the Firmware and Software Version 151
24.2 Licenses 152
24.2.1 System License 153
24.2.2 Application Licenses 154
24.3 Viewing Active Connections 155
24.4 PTZ Overview 156
24.5 Logs 157
24.5.1 About Logs 157
24.5.2 Saving a Log 159

24.5.3 Example of a Log Record 159
24.5.4 Example of an Event Record 159
24.5.5 Example of a Command Record 161
24.6 Hard Disks 162
24.6.1 Information 162
24.6.2 Mount Points 162
24.6.3 Harddisks 162

Appendix A: Abbreviations 163

1 About this Manual

1.1 What is XOa 3?

XOa stands for Xtralis Operating system ADPRO. It consists of the firmware that runs on the ADPRO FastTrace 2 Series (server) and the XOa client software that you install on your pc.

The XOa client software is suitable for the ADPRO Remotely Managed Multiservice Gateway (RMG) devices of the FastTrace 2 Series: FastTrace 2, FastTrace 2X, and FastTrace 2E.

Wherever **RMG** or **server** is mentioned in this document, it applies to all the devices above.

1.2 Scope

This user manual covers the following topics:

- Installation of the XOa client software (new systems only)
- Setup and configuration of the server and its peripheral devices in the client software
- Event and alarm transmission
- User management
- Configuration management.

This user manual does not cover:

- Upgrading legacy systems to XOa (server firmware and client software): see *Field Alert #6 – Upgrading to XOa 3*.
- Installation of hardware: see the *FastTrace 2 Series Hardware Installation Manual*.
- Setup and use of the Xapps: see the documentation of the IntrusionTrace, LoiterTrace, SmokeTrace, and ClientTrace applications.
- License and firmware management using Xchange: see the *Xchange Tool User Manual*.

You can find all documentation on the Xtralis Security Solutions Support site www.xtralissecurity.com (logon required).

2 Installing the XOa Client Software

2.1 System Requirements

2.1.1 Hardware

- Core 2 Duo, 1.6 GHz
- 2 GB RAM
- Graphics card that is compatible with DirectX 7

Xtralis recommended to use a graphics card that allows YUV surfaces and hardware stretching. If not, the XOa client software will force the graphics card to GDI mode, which will increase CPU load.

- It is recommended to install the latest drivers of your graphics card.
  For NVIDIA cards, check http://www.nvidia.com.
  For ATI/AMD cards, check http://ati.amd.com
- If necessary, you can always force the client into GDI mode (not recommended, because of CPU load). Add the line 'gdi=1' in the [General] section of the hydra.ini file. The default location for this file is C:\Users*username*\Appdata\Roaming\AdproXOa\ (where *username* is the name of the Windows user that is currently logged on).

Caution!

These minimum system requirements enable you to configure the server from the client software. However, if you want to use HD cameras in optimal quality, these minimum requirements will prove insufficient. Please take into account that double resolution, on average, results in 4 times more performance.
Xtralis advises to test the settings to make sure that your PC can handle your configuration.

Although the XOa 3 software technically allows for 32 IP channels, these 32 channels are only available on FastTrace 2E models with an Intel DH61BE or MiTAC PH10LU motherboard, and 4 GB RAM or more. On other models, maximum 16 IP channels are available.
Furthermore, to use the 32 IP channels, the FastTrace 2E requires a new system license. Use Xchange to install the new license. For instructions, see *Field Alert #6 – Upgrading to XOa 3*.
Remember to purchase and install additional IP licenses if required.

2.1.2 Software

- Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1
- Internet Explorer 8 or higher
- DirectX 7 drivers.

2.2 Preparing Your PC for Installation

2.2.1 Internet Explorer Settings

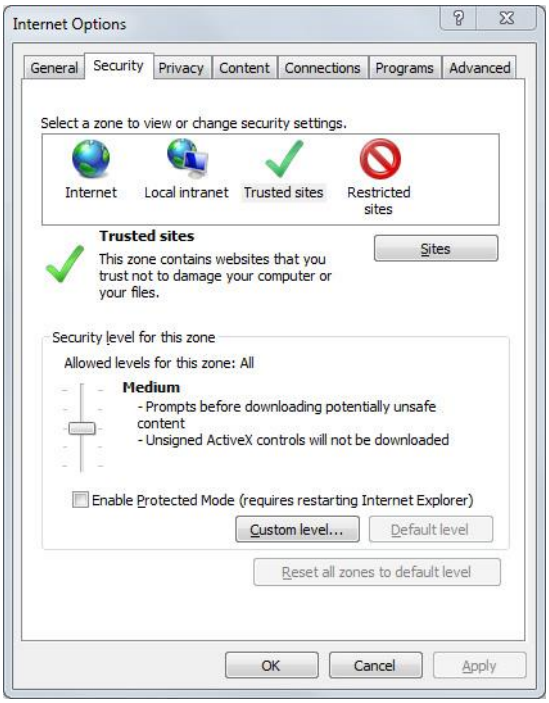
Note

The preferred browser for installing the XOa client software is Internet Explorer. If you cannot use Internet Explorer, try any other internet browser. In this case, you must install the MeadCo Neptune plugin. You can download the plugin from www.meadco.com/Neptune/Download.

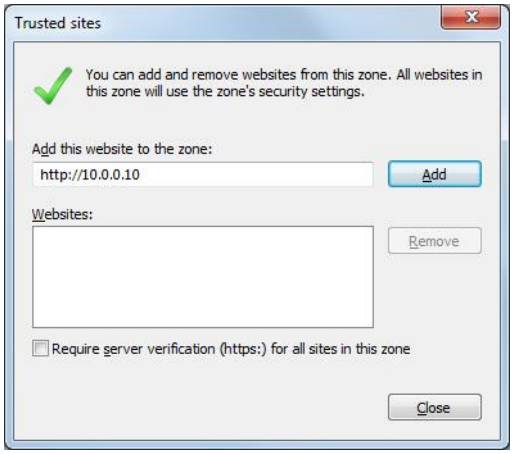
When installing the XOa client software on a **Windows Vista** or **Windows 7** operating system, you need to add the server's IP address to your **Trusted sites** in Internet Explorer. Proceed as follows:

1. In Internet Explorer, choose **Tools > Internet options**.

2. Click the **Security** tab.

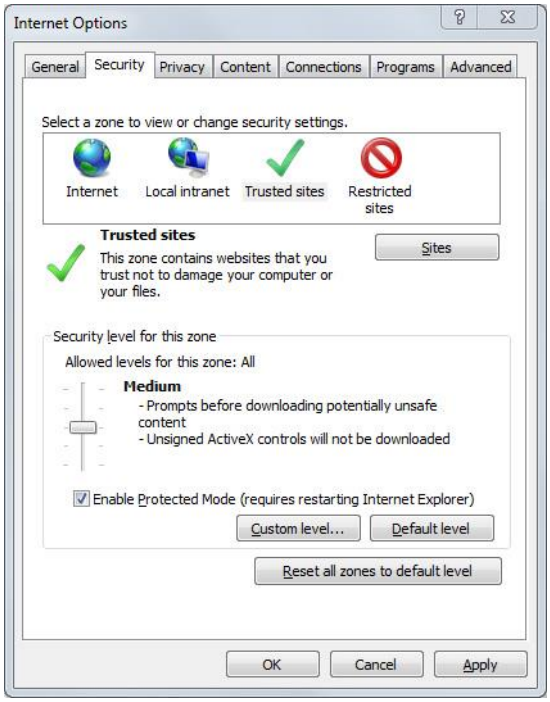


3. In the **Select a zone…** box, click **Trusted** sites, and click **Sites**.


Trusted sites
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Add this website to the zone:
http://10.0.0.10
Add
Websites:
Remove
Require server verification (https:) for all sites in this zone
Close

4. In the **Add this website…** box, type http:// followed by the server's IP address. For example: http://10.0.0.10
5. Click **Add**, and then click **Close**.
6. Click **OK** to close the **Internet Options** window.

If installation is still not possible, you may try clearing the **Protected Mode** check box in the **Security** tab.



Caution!

Check with the IT department if you are allowed to switch off protected mode, because this may cause IT issues.

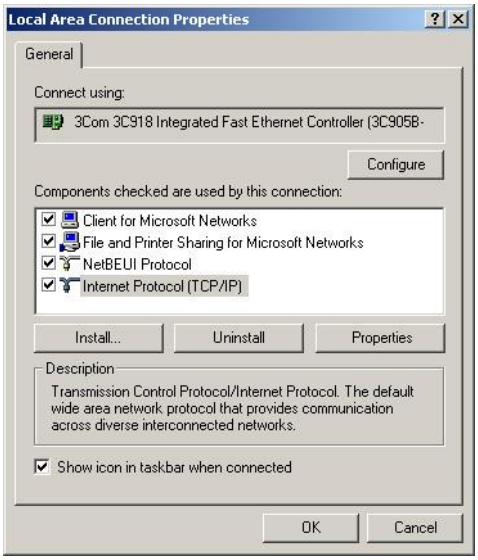
2.2.2 Changing the PC's IP Address

The server's default IP address is 10.0.0.10 with subnet mask 255.255.255.0. When you install the client software, you need to put your PC in the same IP range (e.g. IP address 10.0.0.2 with subnet mask 255.255.255.0).

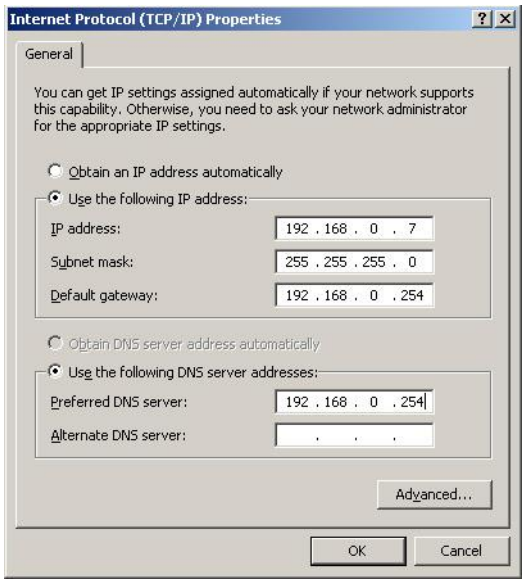
2.2.2.1 In Windows XP

To change the PC's IP address in Windows XP, proceed as follows:

1. Click **Start** and choose **All Programs > Accessories > Communications > Network Connections**.
2. Right-click **Local Area Connection**, and then click **Properties**.



3. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 7
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 254
Alternate DNS server:
Advanced...
OK
Cancel

4. For ease of initial setup, change the PC's TCP/IP settings to the following:

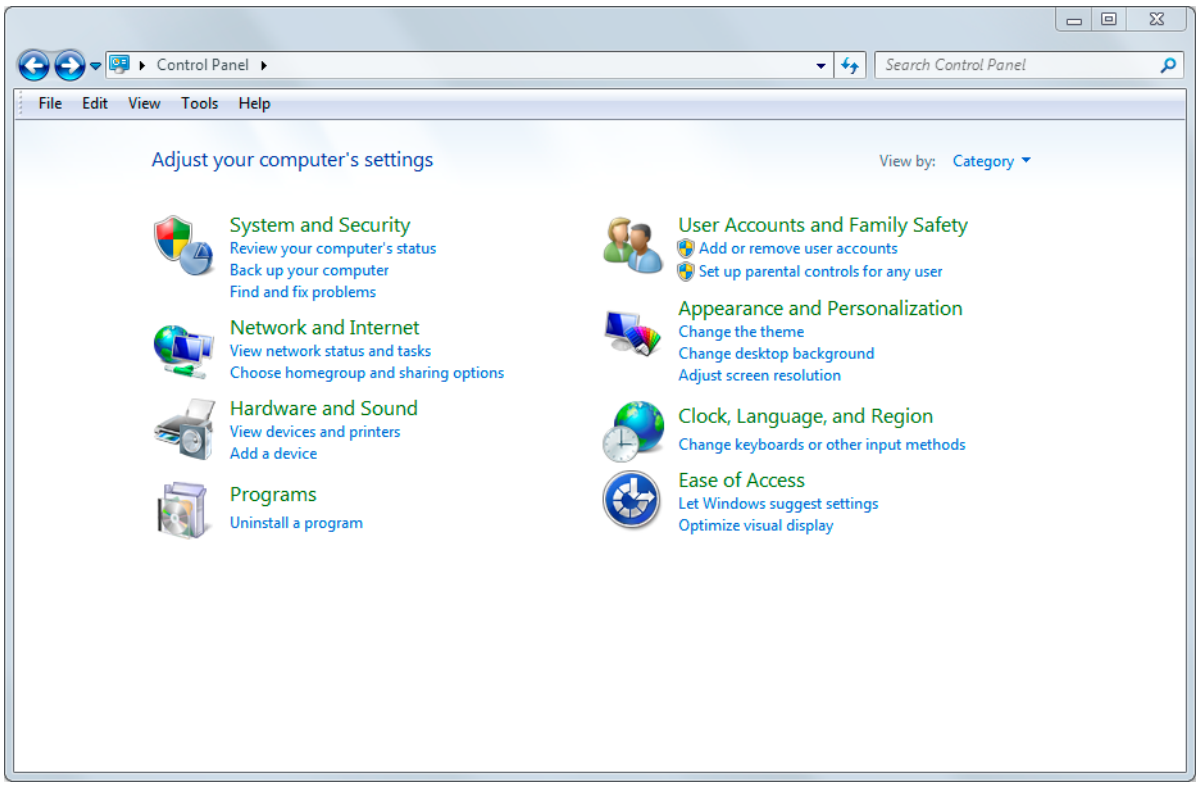
IP address	10.0.0.2
Subnet mask	255.255.255.0

5. Click **OK**. The **Local Area Connection Properties** window appears again.
6. Click **OK**, and then close the **Network and Dial-up Connections** window.

2.2.2.2 In Windows Vista/Windows 7

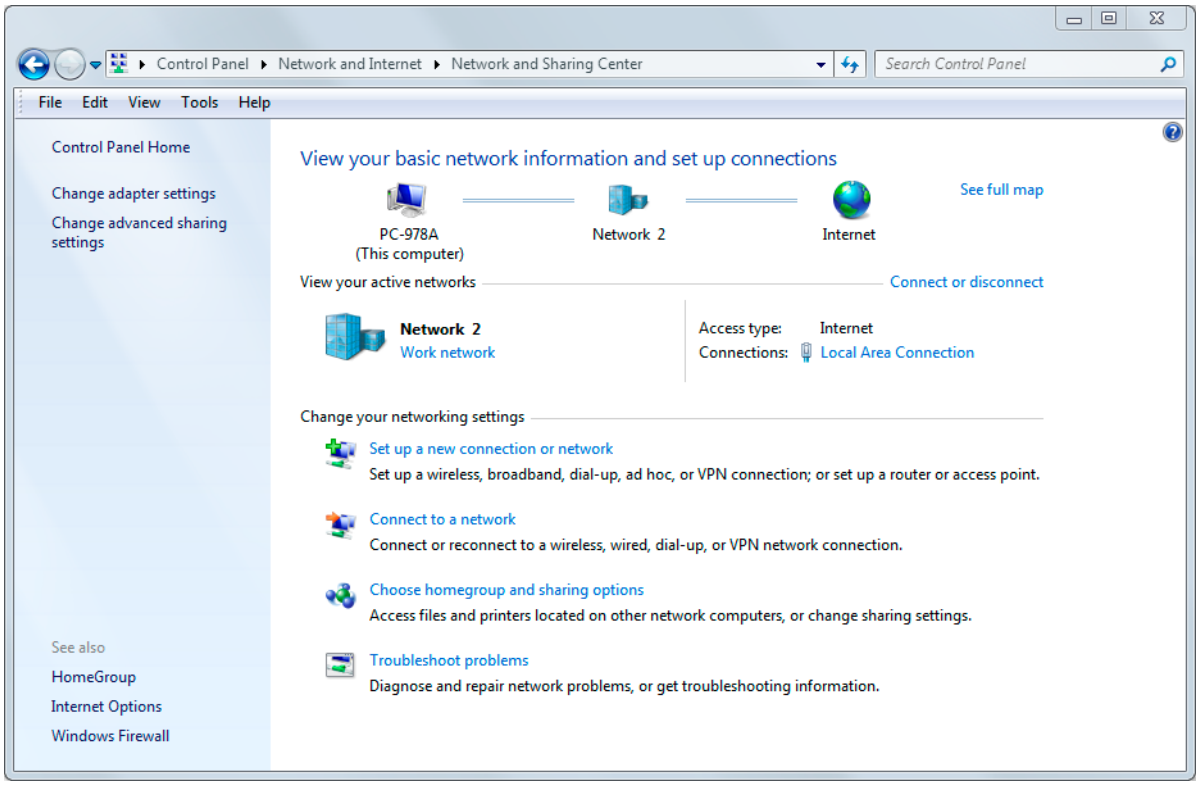
To change the PC's IP address in Windows Vista/Windows 7, proceed as follows:

1. Click **Start**, and then click **Control Panel** (**View by: Category**).

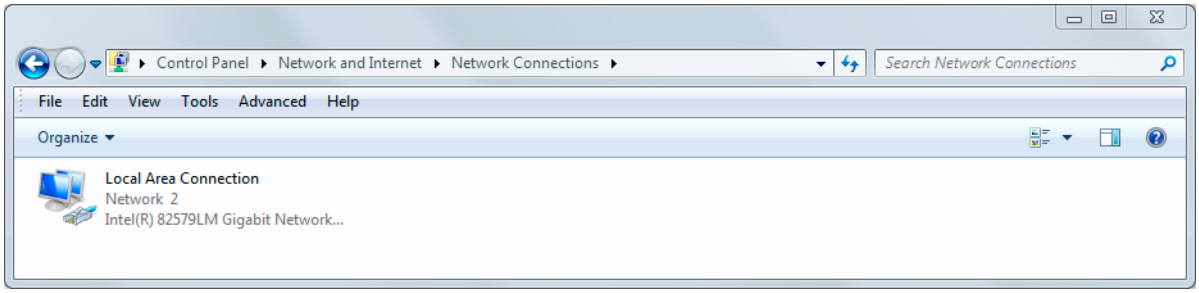


2. Click **Network and Internet**.

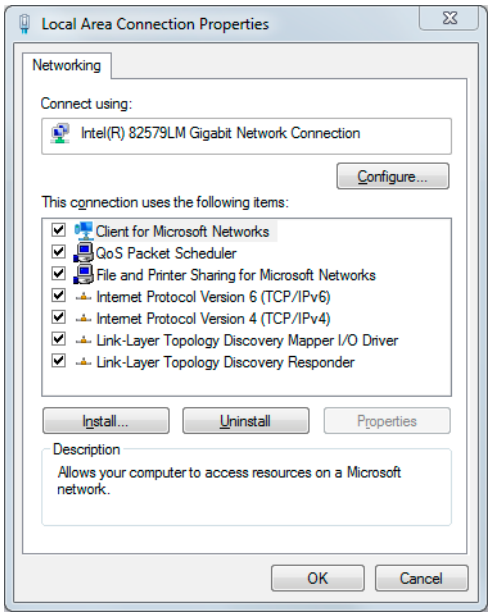
3. Click **Network and Sharing Center**.


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
File Edit View Tools Help
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
PC-978A (This computer)
Network 2
Internet
View your active networks
Connect or disconnect
Network 2
Work network
Access type: Internet
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
HomeGroup
Internet Options
Windows Firewall

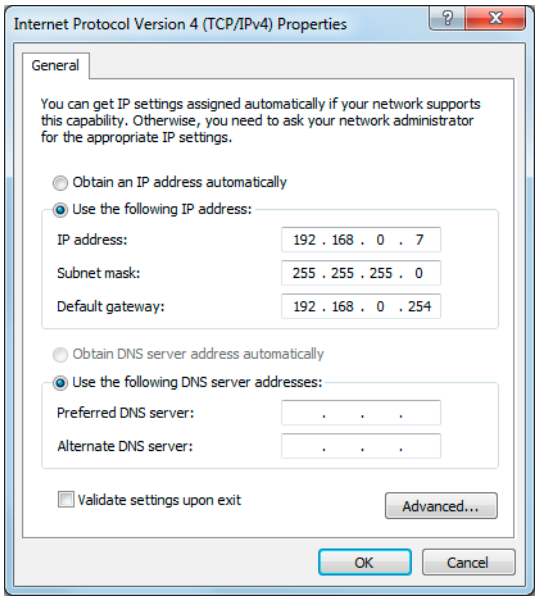
4. Click **Change adapter settings**.


Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Network Connections
File Edit View Tools Advanced Help
Organize
Local Area Connection
Network 2
Intel(R) 82579LM Gigabit Network...

5. Right-click **Local Area Connection**, and then click **Properties**.



6. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 7
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

7. For ease of initial setup, change the PC's TCP/IP settings to the following:

IP address	10.0.0.2
Subnet mask	255.255.255.0

8. Click **OK** to return to the **Local Area Connection** window.
9. Click **OK** to close the window.

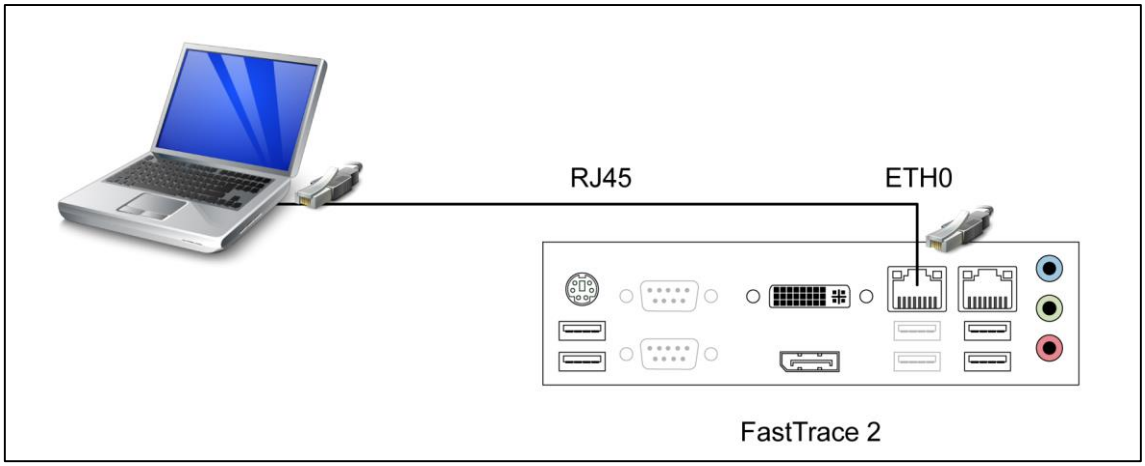
2.3 Installing the XOa Client Software

> ***Note***
>
> The procedure below describes how to install the XOa client software **on a new system**. For **upgrading** your legacy FastTrace 2 server, see *Field Alert #6 – Upgrading to XOa 3*.

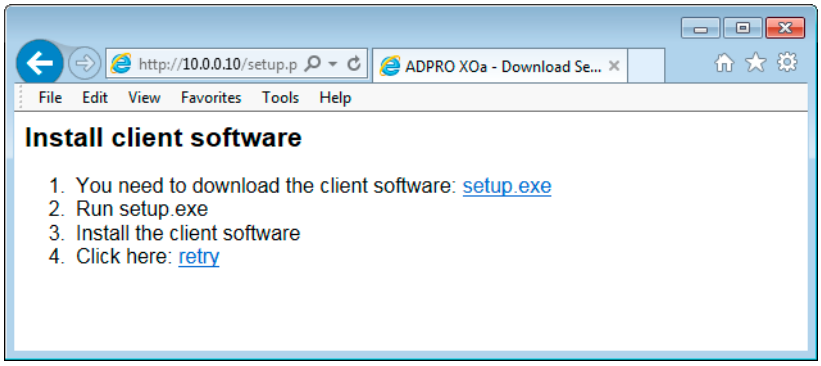
To install the XOa client software, proceed as follows:

1. Connect your PC to the server's ETH0 port with an RJ45 network cross cable or via the network switch/router on the ETH0 port.

> ***Note***
>
> The illustration below shows a server with a MiTAC PH10LU motherboard. To locate the ETH0 port on systems with Intel motherboards, see the *FastTrace 2 Hardware Installation Manual*.



2. Open Internet Explorer and enter the server's IP address, followed by /setup.php
For example:
http://10.0.0.10/setup.php

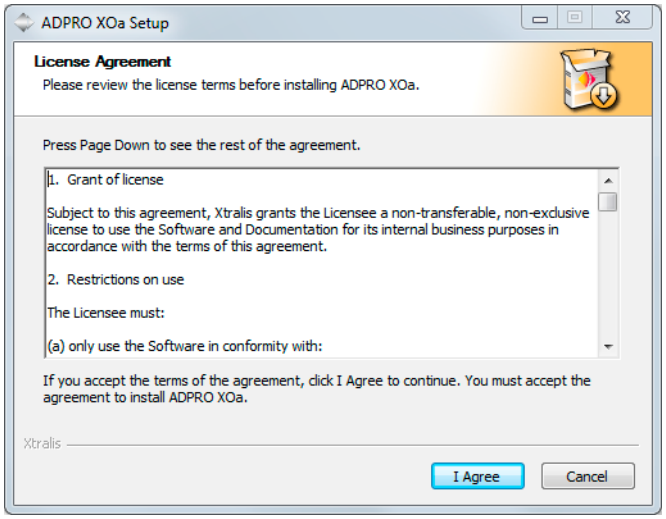

http://10.0.0.10/setup.p
ADPRO XOa - Download Se...
File Edit View Favorites Tools Help
Install client software
1. You need to download the client software: setup.exe
2. Run setup.exe
3. Install the client software
4. Click here: retry

3. Click **setup.exe**.

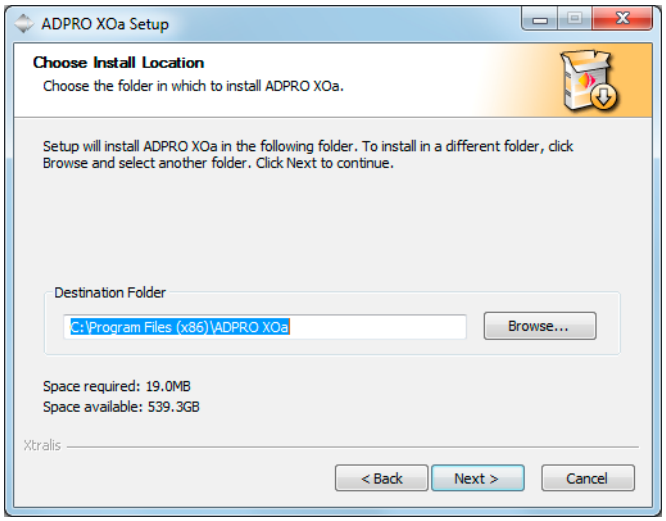
4. Click **Run** to start the installation.

> ***Note***
>
> Your virus scanner may block this download. Disable your virus scanner temporarily if this occurs. Remember to switch it back on after installation.

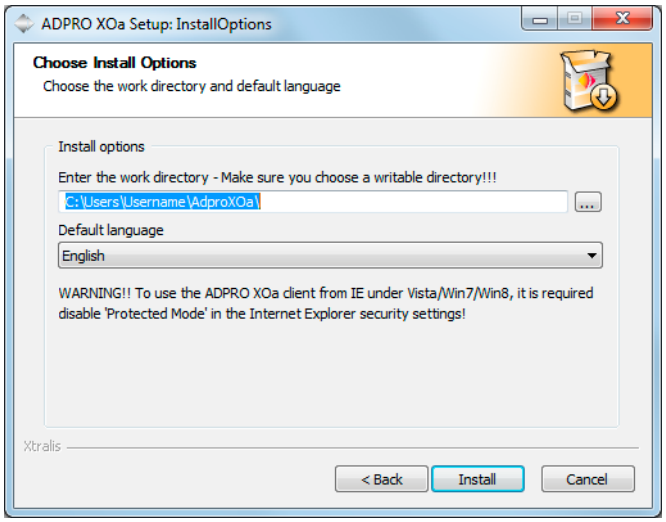
5. The following warning message may appear:
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Click **Yes** to start the installation.


ADPRO XOa Setup
License Agreement
Please review the license terms before installing ADPRO XOa.
Press Page Down to see the rest of the agreement.
1. Grant of license
Subject to this agreement, Xtralis grants the Licensee a non-transferable, non-exclusive license to use the Software and Documentation for its internal business purposes in accordance with the terms of this agreement.
2. Restrictions on use
The Licensee must:
(a) only use the Software in conformity with:
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install ADPRO XOa.
Xtralis
I Agree
Cancel

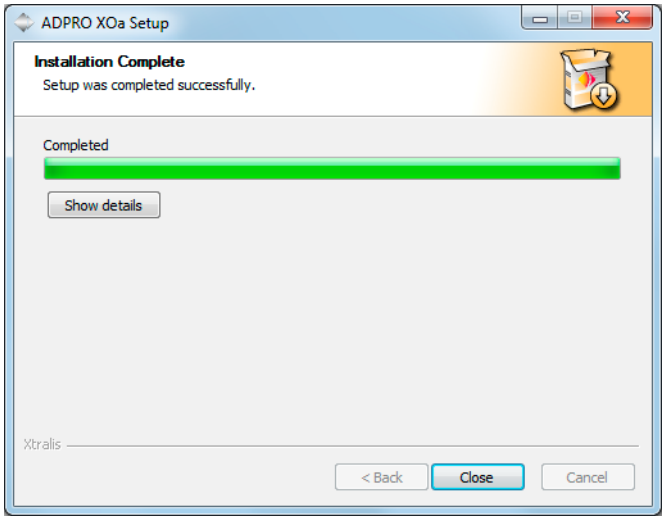
6. Click **I Agree** to agree with the terms of the license agreement.


ADPRO XOa Setup
Choose Install Location
Choose the folder in which to install ADPRO XOa.
Setup will install ADPRO XOa in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Program Files (x86)\ADPRO XOa
Browse...
Space required: 19.0MB
Space available: 539.3GB
Xtralis
< Back
Next >
Cancel

7. Accept or modify the installation folder. Click **Next**.


ADPRO XOa Setup: InstallOptions
Choose Install Options
Choose the work directory and default language
Install options
Enter the work directory - Make sure you choose a writable directory!!!
C:\Users\Username\AdproXOa\
Default language
English
WARNING!! To use the ADPRO XOa client from IE under Vista/Win7/Win8, it is required disable 'Protected Mode' in the Internet Explorer security settings!
Xtralis
< Back
Install
Cancel

8. Accept or modify the work folder (= the folder for storing snapshots and downloaded recordings). Also select your preferred language. Click **Install**.



9. When the installation is completed, click **Close** to exit the installation Wizard.

Note

You cannot access the system page to alter the settings when your client software version is a lower version than the corresponding firmware version on the server! It is recommended practice to have both versions equal.

2.4 Launching and Initial Configuration

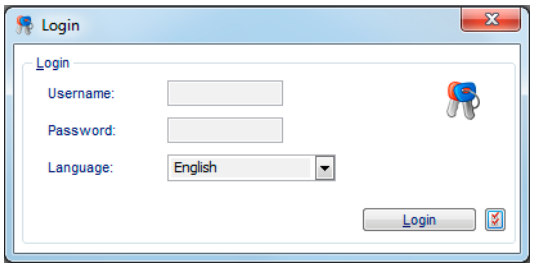
You can launch the XOa client:

- From Internet Explorer
- In its own window (recommended).

2.4.1 Launching the XOa Client in Internet Explorer

To launch the XOa client in Internet Explorer, proceed as follows:

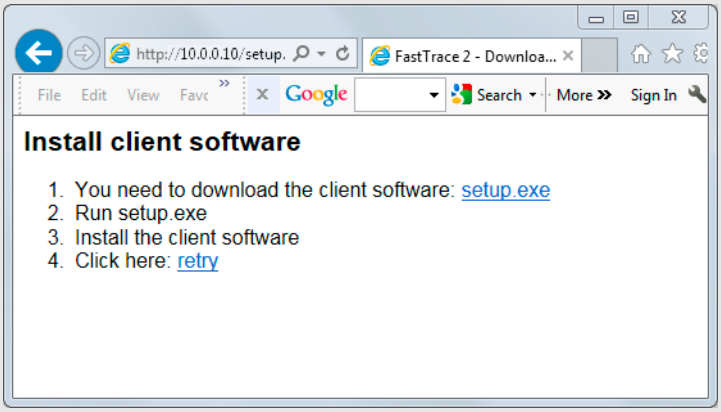
1. Open Internet Explorer and type the server's IP address in the address bar (the default IP address is 10.0.0.10). The login screen appears:



2. Enter the user ID/username and password of an existing user to log on to the server. The default user ID is **0** and the default password is **666777**.
3. In the **Language** box, select the desired language for the application.
4. If required, you can still change the work folder (= the folder for storing snapshots and downloaded recordings): click and set the desired folder.
5. Click **Login**.

Note

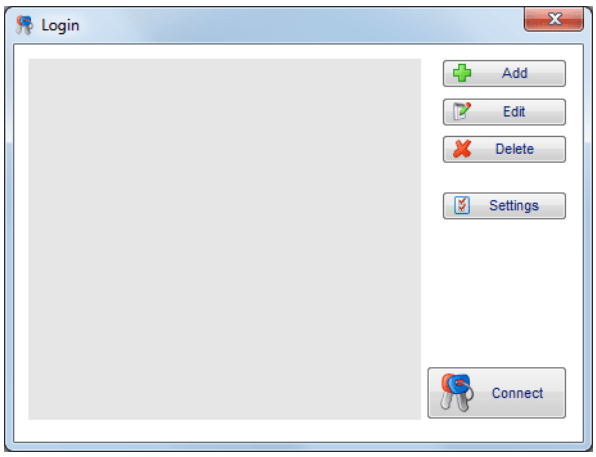
It might occur that – even after the client has been installed – the internet browser is opened instead of the login screen. If this is the case, just click **Retry**.



2.4.2 Launching the XOa Client in Its Own Window

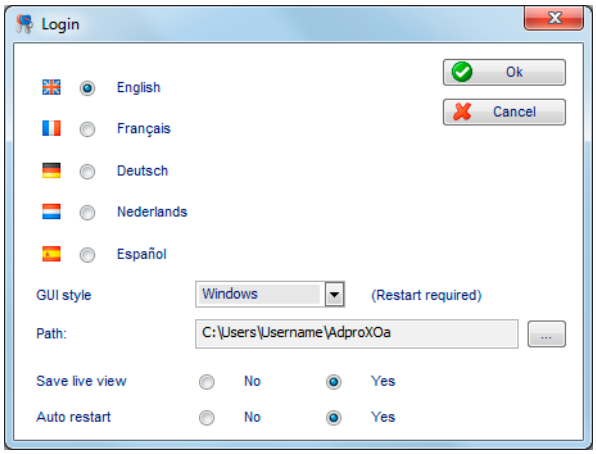
To launch the XOa client in its own window, proceed as follows:

1. On the desktop, double-click the XOa client icon .
   If the icon is not available, you can click **Start** and choose **All Programs > Xtralis > ADPRO XOa > AdproXOa**. The following window appears:



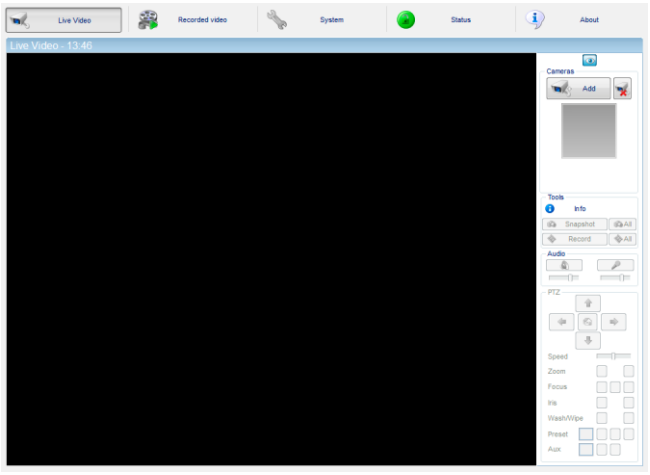
   The **Login** window displays all your servers so that you can quickly connect to them. When using the XOa client for the first time, the list is empty.

2. To set up how the client launches, click **Settings**.



3. Select the desired language for the application.
4. In the **GUI style** box, select a style to change the appearance of the application.
5. If required, in the **Path** box, change the work folder (= the folder for storing snapshots and downloaded recordings).
6. Set **Save live view** to **Yes** if you want to show the last used camera matrix in live view. If you set it to **No**, the live view window is empty when you start the client, and you have to select the cameras for the live view matrix each time you start the client.
7. Set **Auto restart** to **Yes** if you want the login window to reappear when you close the client software. This allows you to quickly connect to another server.
8. Click **OK** to save the settings.

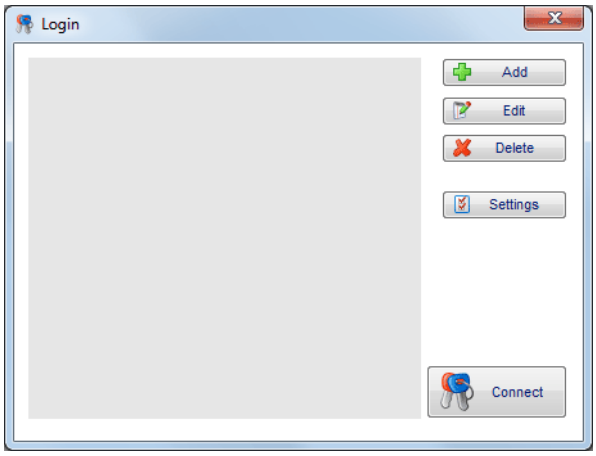
9. To connect the client to a server, click the server in the list, and then click **Connect**. The **Live Video** screen appears:



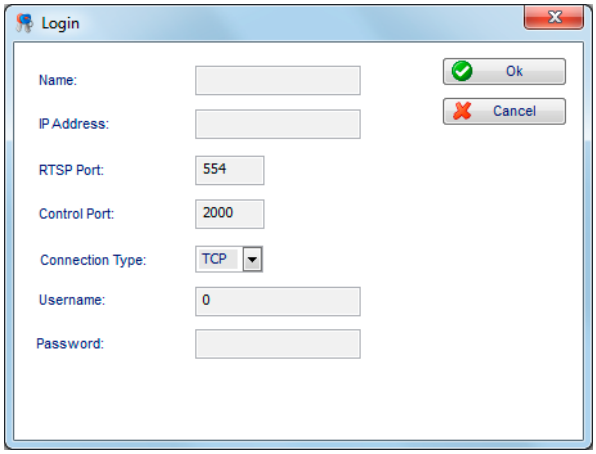
2.4.3 Adding a Server to the XOa Client

To add a server, proceed as follows:

1. Launch the XOa client (in its own window).



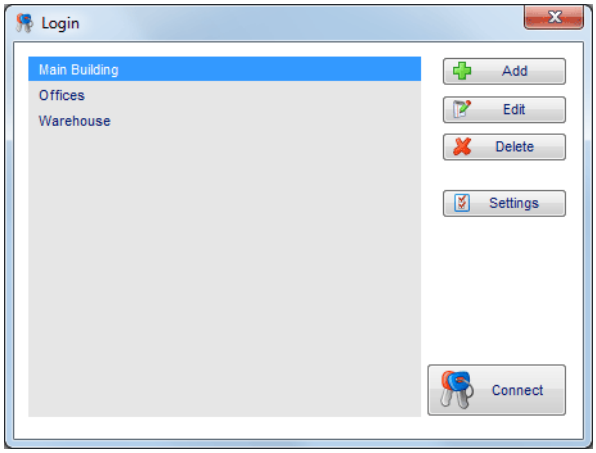
2. Click **Add**. The following window appears:



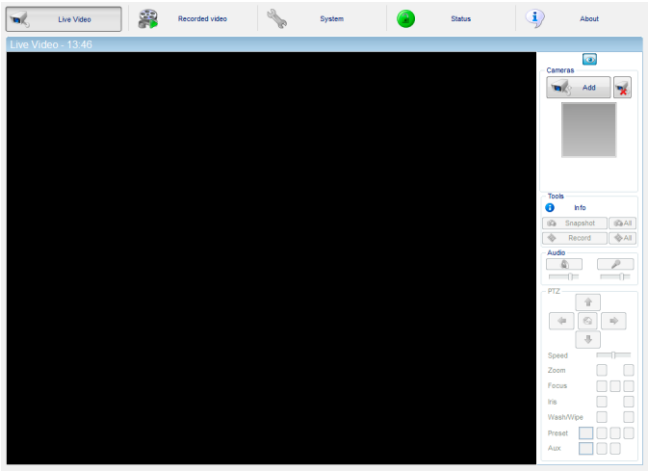
3. Provide the following information:
   - In the **Name** box, type a meaningful name for the server.
   - In the **IP Address** box, type the IP address or DNS hostname of the server (default is 10.0.0.10).
   - Enter the **RTSP Port** (default is 554) and **Control Port** (default is 2000). Use the same ports as specified in the client software under **System > Connections > Ethernet/PPP**. For more information, see *Ethernet Connection* on page 26.

- In the **Connection Type** box, select the TCP or UDP protocol. UDP is recommended, but TCP may be required if the connection goes through a router that blocks the UDP packets.
- Enter the user ID/username and password of an existing user to log on to the server. The default user ID is **0** and the default password is **666777**.

4. Click **OK**. The new server appears in the list.
5. Repeat for any other servers that you want to add.



6. To connect the client to a server, click the server in the list, and then click **Connect**. The **Live Video** screen appears:



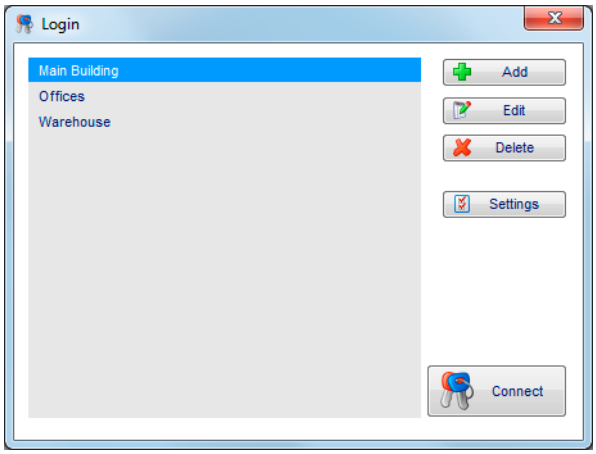
Note

The information about the connected servers within your XOa client software is stored in the HydraApp.ini file. The default location for this file is C:\Users*username*\Appdata\Roaming\AdproXOa\ (where *username* is the name of the Windows user that is currently logged on). Copy/paste this file to any other PC and/or other PC user to obtain the same connected devices without having to add all the servers again.

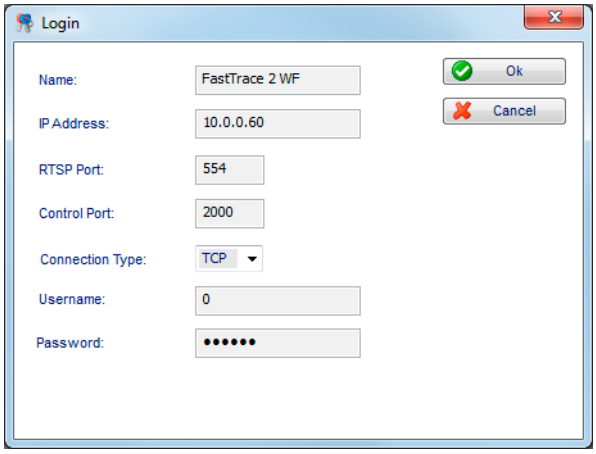
2.4.4 Changing a Server

The first time you connect to a server, you use the default values. If you have modified any settings in the client (IP address, ports, password…), you also have to change these in the **Login** screen. To change a server, proceed as follows:

1. Launch the XOa client (in its own window).



2. Select the desired server in the list, and then click **Edit**.



3. Change the necessary settings.
4. Click **OK** to confirm.

2.4.5 Setting Date and Time

The first time that you connect to a server, set the date and time. This ensures that the correct timestamp appears on recordings and logs.

Changing the date/time settings requires a system restart.

Caution!

If you turn back the clock, the system may erase existing recordings. For example, you need to turn the clock back from 16:00 h to 15:30 h. Any existing recordings that were already made between 15:30 h and 16:00 h may be erased after you set the clock back to 15:30 h.

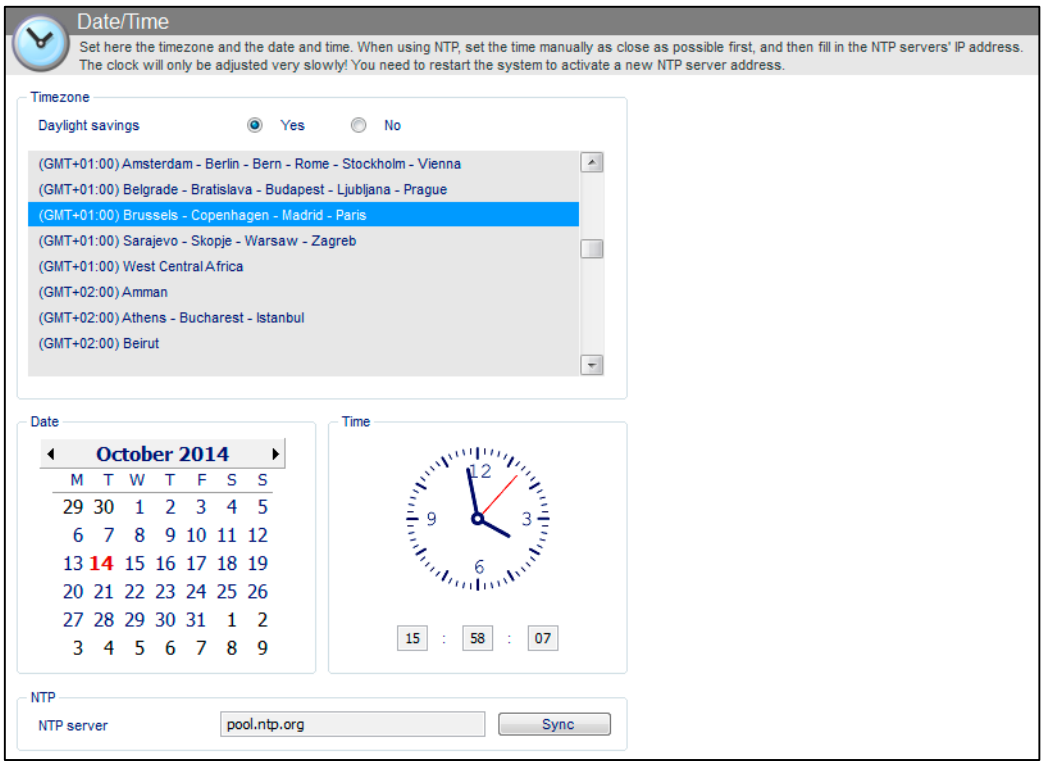
If available, you can let the server synchronise with an NTP server (Network Time Protocol server).

Note

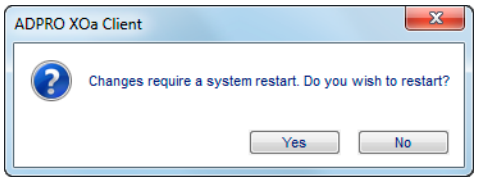
If you experience any instability with the NTP server when using a dynamic NTP address, then enter the DNS server of your Internet Service Provider in the advanced settings for the Ethernet connection: choose **System > Connections > Ethernet/PPP**, click **Advanced mode**, and fill in the **Provider DNS Server** box.

To set the date and time, proceed as follows:

1. Choose **System > General > Date/Time**.


Date/Time
Set here the timezone and the date and time. When using NTP, set the time manually as close as possible first, and then fill in the NTP servers' IP address.
The clock will only be adjusted very slowly! You need to restart the system to activate a new NTP server address.
Timezone
Daylight savings
Yes
No
(GMT+01:00) Amsterdam - Berlin - Bern - Rome - Stockholm - Vienna
(GMT+01:00) Belgrade - Bratislava - Budapest - Ljubljana - Prague
(GMT+01:00) Brussels - Copenhagen - Madrid - Paris
(GMT+01:00) Sarajevo - Skopje - Warsaw - Zagreb
(GMT+01:00) West Central Africa
(GMT+02:00) Amman
(GMT+02:00) Athens - Bucharest - Istanbul
(GMT+02:00) Beirut
Date
October 2014
M T W T F S S
29 30 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 1 2
3 4 5 6 7 8 9
Time
12
3
6
9
15 : 58 : 07
NTP
NTP server
pool.ntp.org
Sync

2. To switch automatically between summer and winter time, set **Daylight savings** to **Yes**.
3. Click the correct time zone in the list.
4. In the **Date** box, click the correct date.
5. In the **Time** box, type the correct time in hours, minutes, and seconds. Enter the time in 24 h notation.
6. If you want to use an NTP server to synchronise time: in the **NTP server** box, type the NTP server's IP address, or its dynamic name.
7. Click **Save**. The following message appears:



8. Click **Yes** and wait for the system to reboot.

3 Connections

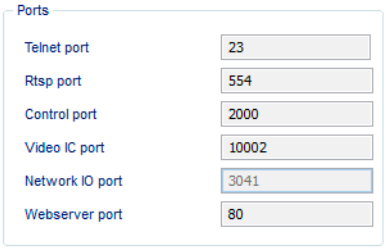
3.1 Network and Modem (Ethernet/PPP)

You can connect the server to a local network or to a remote (PPP dial-in) network, applying an external modem.

To set up the network connections, open **System > Connections > Ethernet/PPP**. Modify the settings and click **Save**.

3.1.1 Ports

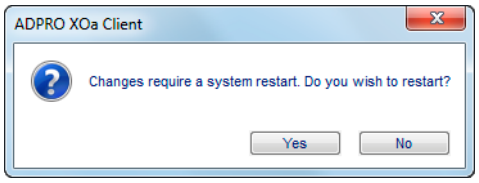
In this section you can set the ports that will be used.



Port	Description	Default value
Telnet port	The IP port used to make a Telnet connection.	23
Rtsp port	Real-time streaming protocol: the client uses this port to control the video streaming. You have to use the same value here as the value specified when adding this video system in the XOa client! (For more information, see *Adding a Server to the XOa Client* on page 21.)	554
Control port	IP port used to exchange information between the server and the XOa client software. (e.g. display status of inputs and outputs) You have to use the same value here as the value specified when adding this video system in the XOa client! (For more information, see *Adding a Server to the XOa Client* on page 21.)	2000
Video IC port	Port used to interconnect with S3100 security panels. This allows starting a recording on an alarm detected on the security panel. Use the same port as the one selected in the S3100 configurator!	10002
Network I/O port	Port used to poll the Net I/O modules. This port is fixed, you cannot change it.	3041
Webserver port	Port used for the http protocol.	80

We strongly recommend using the default ports. If this is not possible, please document the use of the new ports thoroughly.

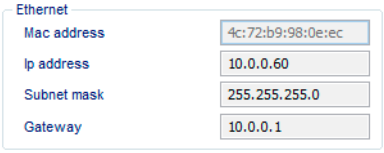
If you change some settings, you may have to restart the server:



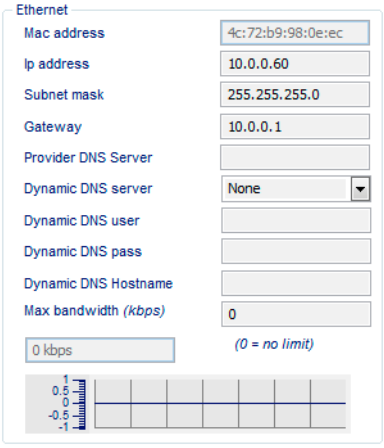
Click **Yes** to restart the video system and apply the new settings.

3.1.2 Ethernet Connection

Enter all necessary information for the Ethernet connection in this section.

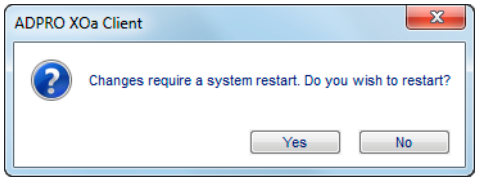


Click **Advanced mode** to define the Dynamic DNS settings.



Parameter	Description	Default value
MAC address	Shows the MAC address of your video system.	–
IP address	Enter the IP address of the server. Do not use reserved addresses!	10.0.0.10
Subnet mask	Enter the subnet mask.	255.255.255.0
Gateway	Set the gateway (= IP address of the router).	10.0.0.1
Provider DNS server	Enter the provider DNS server. The server needs this information to be able to connect to the Dynamic DNS server. When using internet over Ethernet this field is optional, because certain protocols have been programmed in the software, when the internet connection is only available via a 3G modem (in the PPP section), this field is obligatory.	–
Dynamic DNS server	Choose the correct provider from the list. ***Note*** First the Dynamic DNS account (with any Dynamic DNS service provider) needs to be set up.	None
Dynamic DNS user	Enter the username you have received from your provider for the Dynamic DNS account.	–
Dynamic DNS pass	Enter the password you have received from your provider for the Dynamic DNS account.	–
Dynamic DNS host	Enter the host you have received from your provider for your Dynamic DNS account.	–
Max. bandwidth	This limits the total bandwidth used by the video system. This may affect image rate, but not the image quality, during live viewing. The value is expressed in kbps.	–
Currently used bandwidth	This shows the current bandwidth usage, both the value and the graphical view. The value is expressed in kbps.	–

If you change some settings, you may have to restart the server:



Click **Yes** to restart the video system and apply the new settings.

3.1.2.1 Configuring Dynamic DNS Settings

Enter the required parameters – either in the Ethernet or the PPP section – and click Save. Wait about 10 seconds. If an error occurs during the connection to the Dynamic DNS service, an error window will pop up. At the same time, the alarm 0055 – [SYST] – DYN DNS FAILED will be set. This alarm can be viewed in the Status window. Faults can be due to a faulty login, wrong password, or wrong host name.

To register to a Dynamic DNS service provider, the server needs access to the internet and to a DNS server to resolve the host name of the service provider. This internet connection can be provided by the Ethernet connection or a 3G connection. When the internet connection is only available through 3G, it is necessary to enter the correct Provider DNS server in the Ethernet section!

Note

- If you configure a Dynamic DNS service for both the Ethernet and the PPP (3G) connection, it is necessary to use different host names (only 1 account required, 2 host names).
- When the RMG is behind a router, the external IP address will be used by the Dynamic DNS service. This will automatically be set by the RMG, so no changes in the XOa settings are necessary.

3.1.2.2 Dynamic DNS Error Messages

3.1.2.2.1 Warning: Unable to determine IP address

If you receive this error message, the RMG could not resolve the service provider's host name. Please check the DNS server in the Ethernet section or check the internet connection of the RMG .

3.1.2.2.2 No update required

If you change settings for the Dynamic DNS, the RMS server will write a new configuration and force an update of this configuration. Some service providers may return a message such as "No update required" or "Attempts to change to the current address are considered abusive". This alarm will automatically reset on the next automated check after one minute.

Note

An error message is displayed only once. If you want to view the message once again, set the Dynamic DNS server to None, click Save, then re-enter your DNS provider and click Save again. Wait a few seconds and the message will reappear.

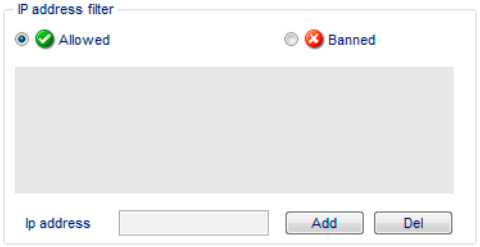
3.1.2.3 Why Use Dynamic DNS?

Dynamic DNS provides the capability for a networked device, such as a router or modem, to notify a Domain Name System (DNS) to change, in real time, the active DNS configuration of its configured hostnames, addresses, or other information. Thus a hostname can be used instead of the IP address, which is very interesting for DHCP attributed IP addresses. Especially with 3G the IP address is often attributed by DHCP.

It also becomes possible to automatically update the client software.

3.1.3 Granting Access to the Server

To limit the access to the video system, you can either enter a list of authorized clients (the green option) or a list of non-authorized clients (the red option). Your choice of course depends on the specific situation. This is only displayed in the *Advanced mode*.



Click **Add** to add an IP address to the selected list.

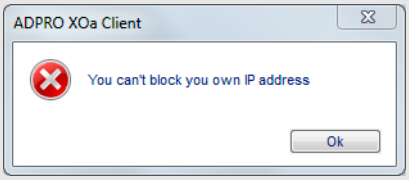
Note

You **cannot** use both lists at the same time.

Important remark:

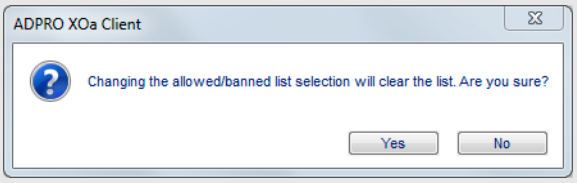
For security reasons the IP address of your PC on which the XOa client software is running, is by default added to the *Allowed* list when you add any other IP address. If this were not the case, you would be blocked out from your own PC.

When you clear the *Allowed* list again, you will get the message that it is impossible to delete the own IP address.



However, if you only leave your own IP address in the Allowed list, no other client (on a computer with another IP address) will be able to connect to the server.

If you want to fully clear the *Allowed* list, just select the *Banned* list, and click **Yes** when asked if you want to clear the list.

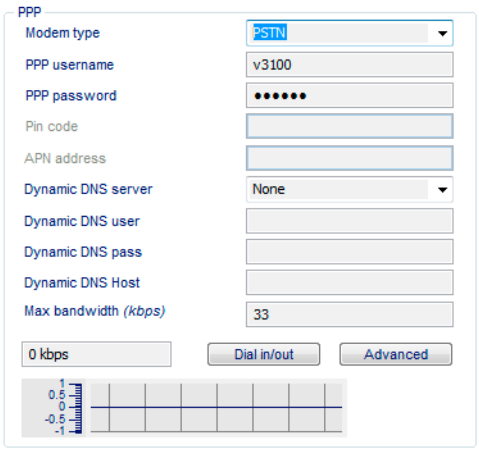


3.1.4 PPP Connection

You need to access the Advanced mode to be able to configure the PPP settings!

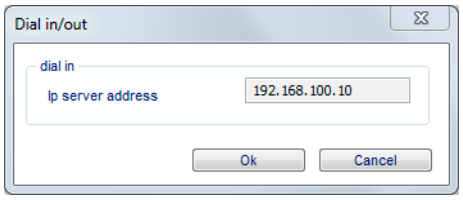
3.1.4.1 PSTN or ISDN Modem Configuration

If you have connected a PSTN or ISDN modem to the server, choose the option PSTN for modem type in the PPP section.



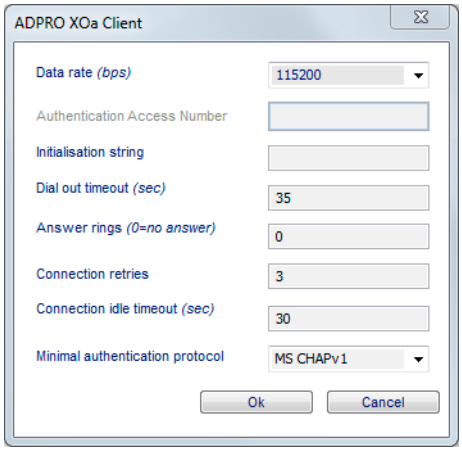
Parameter	Description	Default value
Modem type	Set the modem type to PSTN when using a standard modem that uses the analogue line (AT modem) or digital line (ISDN). The modem should always be connected to the first USB port /dev/ttyU1.	None
PPP username	The login username of a user allowed to connect to the dial-in network (PPP authentication).	V3100
PPP password	The login password of a user allowed to connect to the dial-in network (PPP authentication).	666777
Dynamic DNS server	Choose the correct provider from the list. ***Note*** First the Dynamic DNS account (with any Dynamic DNS service provider) needs to be set up.	None
Dynamic DNS user	Enter the username you have received from your provider for the Dynamic DNS account.	–
Dynamic DNS pass	Enter the password you have received from your provider for the Dynamic DNS account.	–
Dynamic DNS host	Enter the host you have received from your provider for your Dynamic DNS account.	–
Max. bandwidth	This limits the bandwidth used by the video system. This may affect image rate, but not image quality, during live viewing. The value is expressed in kbps. “0” means no limit.	33 (suitable for V34 modem)
Currently used bandwidth	This shows the current bandwidth usage, both the value and the graphical view. The value is expressed in kbps.	–

Click **Dial in/out** to open this window.



Parameter	Description	Default value
IP server address	This is the IP address that will be assigned to the server when the client establishes a remote connection.	192.168.100.10

Click **Advanced**. The following screen appears:



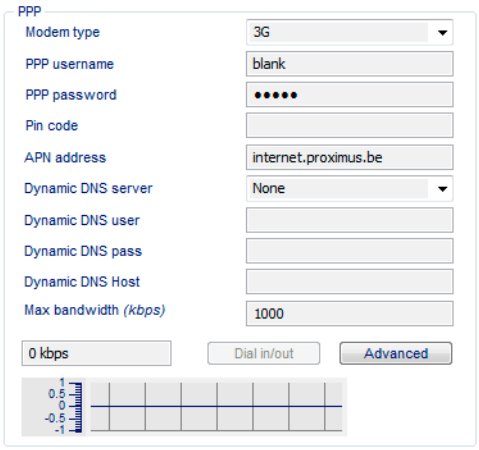
Parameter	Description	Default value
Data rate (bps)	This sets the baud rate of the modem.	115200
Initialisation string	Hayes command string to initialize the modem.	–
Dial out timeout (sec)	This sets the time in which a connection has to be established with the remote client. If not successful, the video system will retry to make the connection. The number of attempts is limited by the parameter “Connection retries”. Be aware that a PPP connection over PSTN can easily take 30 to 60 seconds.	35
Answer rings (0 = no answer)	This sets the number of rings on an incoming call before hooking off.	0 (do not answer any call)
Connection retries	The number of attempts the video system will make to connect to the remote client.	3
Connection idle timeout (sec)	This sets the delay after which the video system will disconnect if no more data is exchanged.	30
Minimal authentication protocol	Selects the authentication protocol that will be used during the setup of a remote connection: PAP/CHAP/MSCHAPv1/MSCHAPv2.	MS CHAPv1

3.1.4.2 3G Modem Configuration

If you have connected a 3G modem to the server, choose the option **3G** for modem type in the **PPP** section.

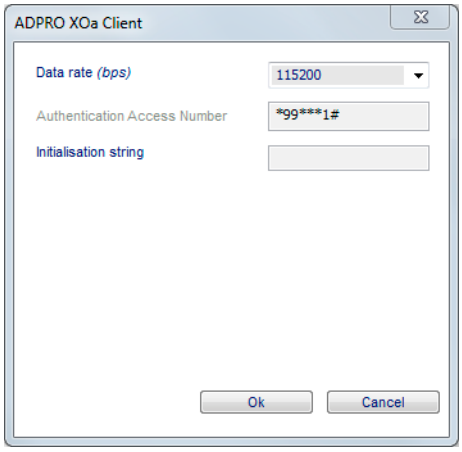
Note

The server supports only the Sierra Wireless Airlink Raven XE modem. Xtralis does not guarantee that any other 3G modem will work properly.



Parameter	Description	Default value
Modem type	Set the modem type to 3G when using a 3G modem.	None
PPP username	The login username of a user allowed to connect to the dial-in network (PPP authentication).	
PPP password	The login password of a user allowed to connect to the dial-in network (PPP authentication).	
Pin code	Enter the pin code for your 3G SIM card.	–
APN address	Enter the APN (Access Point Name) address of your provider.	–
Dynamic DNS server	Choose the correct provider from the list. ***Note*** First the Dynamic DNS account (with any Dynamic DNS service provider) needs to be set up.	None
Dynamic DNS user	Enter the username you have received from your provider for the Dynamic DNS account.	–
Dynamic DNS pass	Enter the password you have received from your provider for the Dynamic DNS account.	–
Dynamic DNS Host	Enter the host you have received from your provider for your Dynamic DNS account.	–
Max bandwidth (kbps)	This limits the bandwidth used by the video system. This may affect image rate, but not image quality, during live viewing. The value is expressed in kbps. “0” means no limit.	1000
Currently used bandwidth	This shows the current bandwidth usage, both the value and the graphical view. The value is expressed in kbps.	–

Click **Advanced**. The following screen appears:

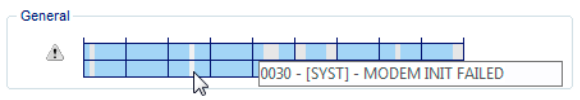


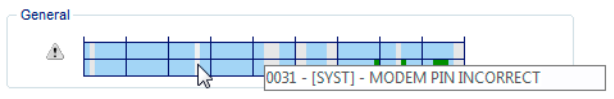
Parameter	Description	Default value
Data rate (bps)	This sets the baud rate of the modem.	115200
Authentication Access Number	This number will be dialled by the 3G modem to setup a data connection. The number depends on the country and/or the provider. E.g.: Vodafone in Australia uses *99***2#.	*99***1#
Initialisation string	Hayes command string to initialize the modem.	

Note

The moment you choose 3G as modem type, and save, the server will automatically search for the internal 3G connection.

To display the progress, the error 0030 – [SYST] – MODEM INIT FAILED appears on the **Status** page. This error message disappears after about 45 seconds (depending on the connection) when the server establishes the 3G connection. If the error message persists, there is a problem with the modem USB connection or the 3G settings. If you have entered an incorrect pin code, the error message 0030 – [SYST] – MODEM PIN INCORRECT appears.





If a 3G connection is set up successfully, but the server cannot establish a connect, then try changing the control port on the Ethernet page. The default control port is 2000, but many providers block it. Changing the control port to port 2001 may resolve the problem.

3.2 IP Camera Network Configuration

3.2.1 General Setup

Servers with an Intel motherboard use an additional network card to access the IP camera network: either a HIPI card or an Ethernet card. The latest models with the MiTAC PH10LU motherboards do not require a separate network card. The setup of the IP camera network is identical for all models.

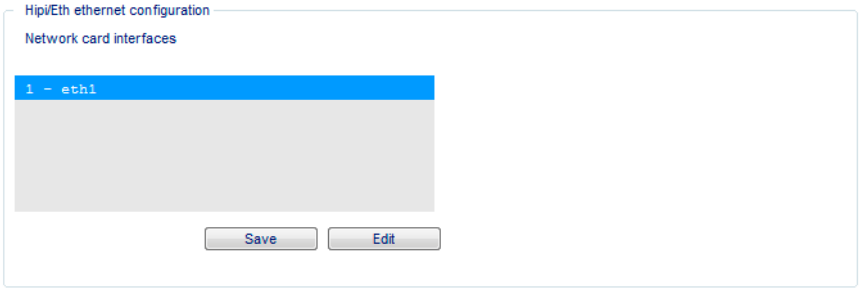
Note

Connect the HIPI/Ethernet card to ETH1 or ETH2 of the server, not to ETH0.

The IP address of your RMG video system and the IP address of the HIPI/Ethernet card must be in different ranges.

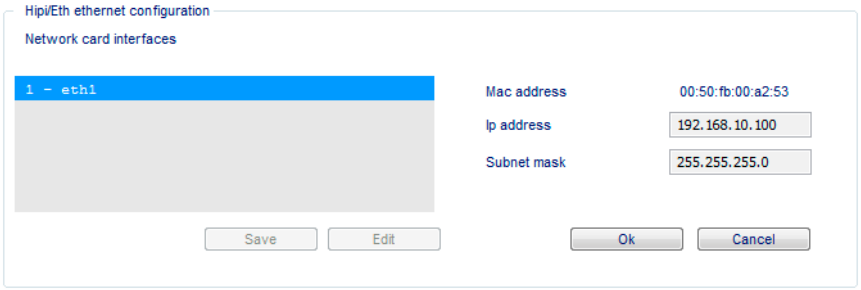
To set up the IP camera network, proceed as follows:

1. Choose **System > Maintenance > Hipi/Eth config**.



   If the server contains two HIPI cards, you see two cards listed. In all other cases, the list only contains **eth1**.

2. Click **eth1**, and then click **Edit**.



3. Enter the IP address and subnet mask.
4. Click **OK**.
5. If the server contains two HIPI cards, repeat for the second card.
6. Click **Save**.
7. Click **Yes** and wait for the system to reboot.

3.2.2 Ethernet Cards

Note

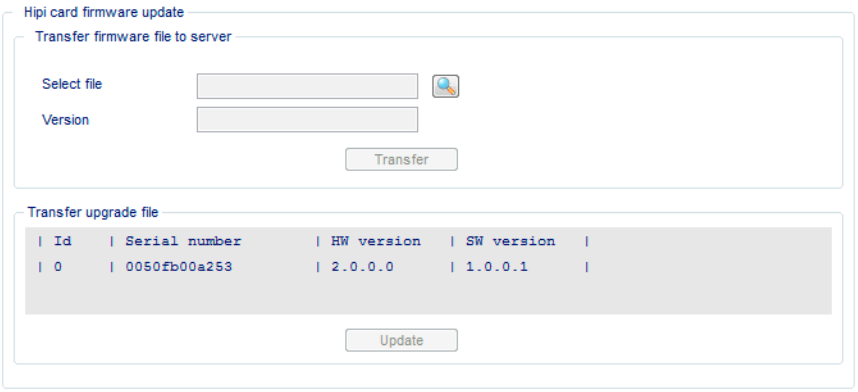
If you receive error message 0080 – [SYST] – DECODER CARD ERROR, your Ethernet card is not functioning correctly. Restart the server. If the error message persists, you need to replace the Ethernet card.

3.2.3 HIPI Cards

Note

If you receive error message 0080 – [SYST] – DECODER CARD ERROR, your Ethernet card is not functioning correctly. Restart the server. If the error message persists, you need to replace the Ethernet card.

The HIPI card requires software. You can check the hardware and software versions of the card in the lower pane of the configuration window. When you buy a new HIPI card, it comes with the latest available software version.


Hipi card firmware update
Transfer firmware file to server
Select file
Version
Transfer
Transfer upgrade file
| Id | Serial number | HW version | SW version |
| 0 | 0050fb00a253 | 2.0.0.0 | 1.0.0.1 |
Update

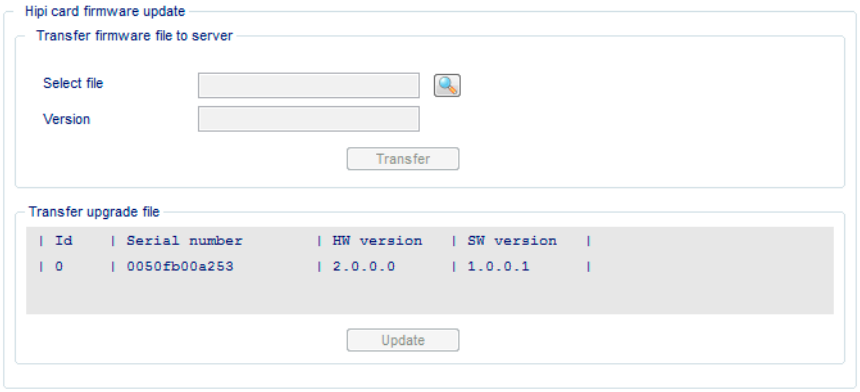
Note

From version 2.9 onwards, you can configure the HIPI card to function as an Ethernet card, providing software decoding of the IP camera streams.

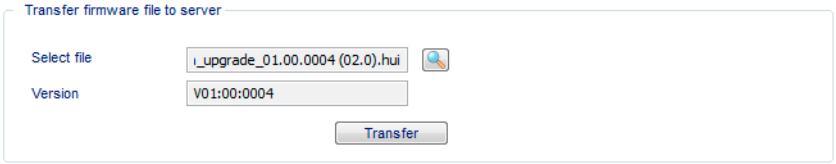
In this case you need to update the HIPI card software with HIPI fpga update file 01.00.0004(02.0).hui.

To update the HIPI card to a more recent version of the software, proceed as follows:

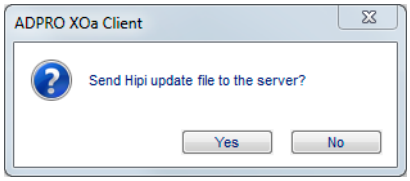
1. Choose **System > Maintenance > Hipi/Eth config**.


Hipi card firmware update
Transfer firmware file to server
Select file
Version
Transfer
Transfer upgrade file
| Id | Serial number | HW version | SW version |
| 0 | 0050fb00a253 | 2.0.0.0 | 1.0.0.1 |
Update

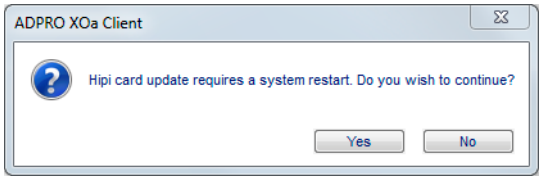
2. Click the button and browse to the .hui upgrade file.
3. Click **Open**. The **Version** box displays the firmware version that you will upload.



4. Click **Transfer**.



5. Click **Yes** to confirm.
6. In the **Transfer upgrade file** panel, click **Update**.



7. Click **Yes** and wait for the system to reboot.

3.3 Audio

3.3.1 Audio IN

For cameras with an audio input, you can choose to record audio and listen to audio in the live view.

Note

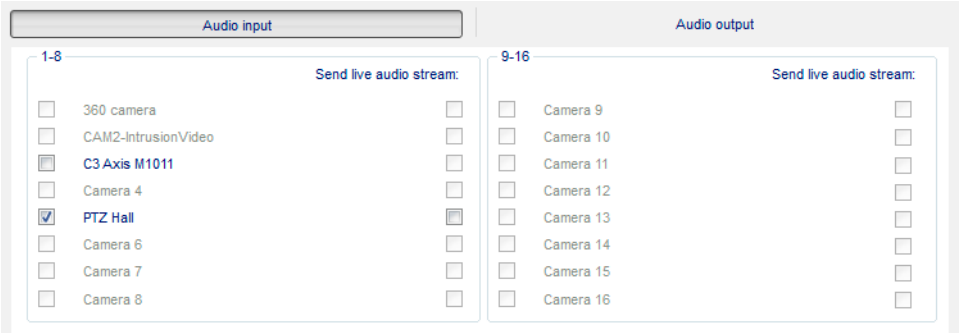
If the connection bandwidth is low, it is recommended to disable live audio streaming.

Audio IN is unbalanced audio.

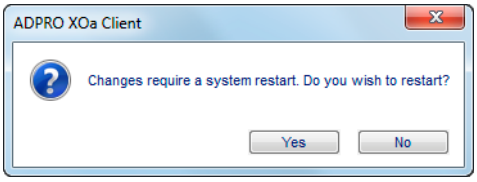
Changing the audio settings requires a system restart.

To enable audio for the cameras, proceed as follows:

1. Choose **System > Connections > Audio**.
2. To record audio for a camera, select the camera's check box. Note that you can only select cameras that have an audio stream available.
3. To enable audio in the live view for a camera, also select the **Send live audio stream** check box.



4. Click **Save**. Changing the audio settings requires a system restart:



5. Click **Yes** to restart the video system and apply the new settings.

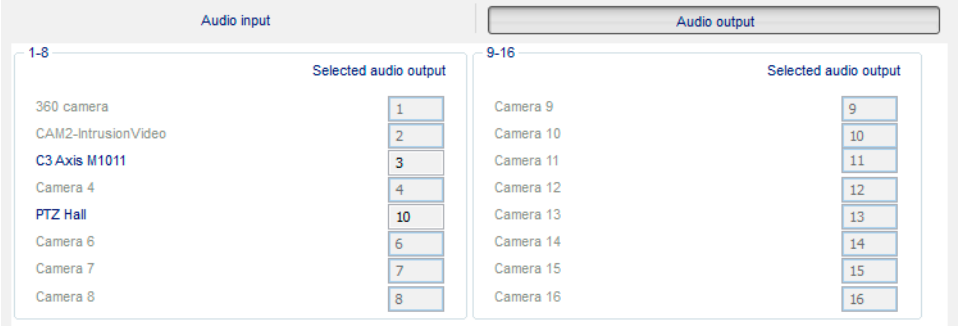
3.3.2 Audio OUT

There is one general audio output available on the server: either via the MIO card or via the audio out plug of the motherboard (= green 3.5 mm jack). If necessary, you can add VM22A audio units.

Audio outputs are available on one or two VM22A units, connected in cascade. Unit 0 is controlled by the MIO card, and drives loudspeakers 1 to 10. Unit 1 connects to the first unit through the EIO loop connector and drives loudspeakers 11 to 20.

(For more information, see the *VM22A Audio Switcher – Installation and User Manual*).

You can assign each loudspeaker to a camera of your choice.



To talk back to a person on the remote site, proceed as follows:

1. In the menu at the top, click **Live Video**.
2. Click the desired camera view. By default the *Push to talk* mode will be active.
3. Click and hold the microphone button .
4. You can now start talking through the microphone that is connected to the MIC input of the computer.

When the option *Full duplex mode* has been ticked, the *Push to talk* mode will be disabled. In this case you can activate the audio by simply clicking the microphone button. To deactivate the audio mode you need to click the button again.

Make sure the audio output parameters are correct. Open **System > Connections > Audio** to modify the settings. Mind that the audio IN option must be activated if you want to use Audio OUT.

Enter the audio server port (by default port 3000) that will be used to transmit audio from the client to the server. Also select the desired protocol (by default UDP) that will be used to transmit the audio.

If you want to force duplex mode to allow simultaneous communication in both directions (not recommended), tick the option **Full duplex mode**. The *Push to Talk mode* will be disabled when this option is ticked.

Click **Save**.

3.4 Internal I/O Cards

OTB I/O (On The Box Inputs & Outputs):

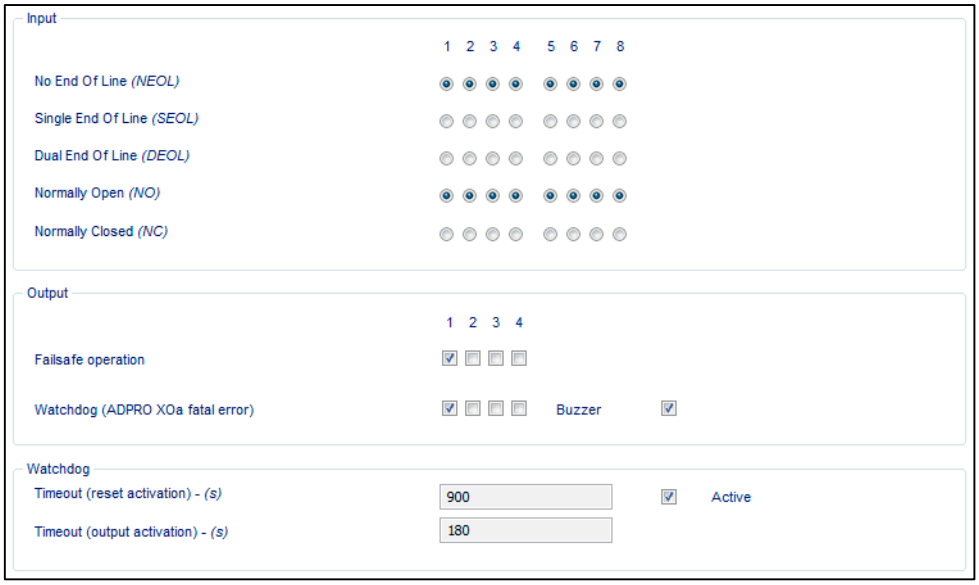
- Internal Main I/O card (MIO) and Extension I/O card (EIO), offering 20 balanced inputs, 8 relay outputs and control signals for either VM22A equipment (audio output switcher) or PTZ cameras (RS-485 output).
- Second set with MIO and EIO card possible to double the number of inputs to 40 and the number of outputs to 16. This also adds an output for PTZ cameras.

The server automatically detects all connected MIO and EIO cards.

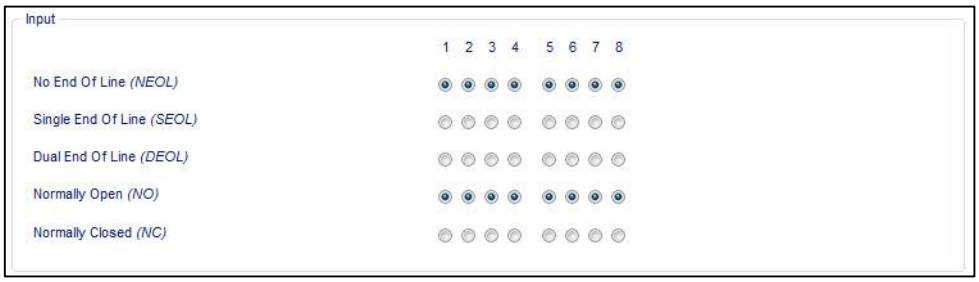
To configure the inputs and outputs in the client software, proceed as follows:

1. Choose **System > Connections > I/O**. The screen shows an overview of the I/O card sets.

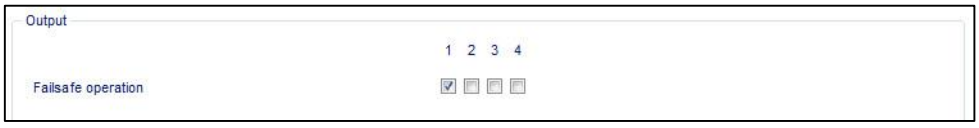
2. Select the desired I/O card set in the list, and then click **Configuration**. The following screen appears:



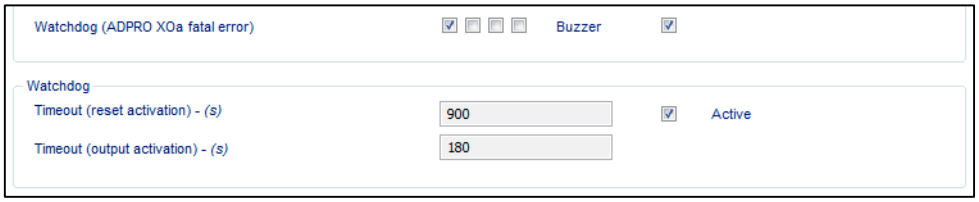
3. For each input, select the correct configuration: NEOL, SEOL, or DEOL; with NO or NC contact. For more information, see the *FastTrace 2 Hardware Installation Manual*.



4. Select the **Failsafe operation** check box for each output that operates in failsafe mode. Failsafe operation means that the relay is activated during idle state, and drops when the output is driven. The advantage is that failsafe outputs drop to ‘alarm state’ when the power supply is cut.



5. Select the **Watchdog** check box for each output that operates in Watchdog mode. Watchdog operation means that the output is activated when the video system cannot reach the I/O card for some time, as specified by **Timeout (output activation)**. This situation can occur when the video system hangs. Timeout values are specified in seconds.



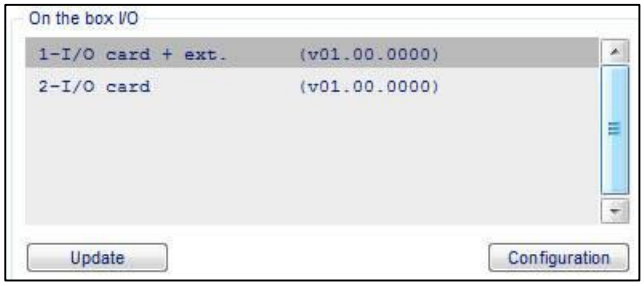
6. If you use the watchdog feature, type the number of seconds after which the system must activate the Watchdog output in the **Timeout (output activation)** box.
7. If you want the buzzer to sound during a watchdog alarm, check the **Buzzer** check box.
8. Click **OK** to save the settings.

Note

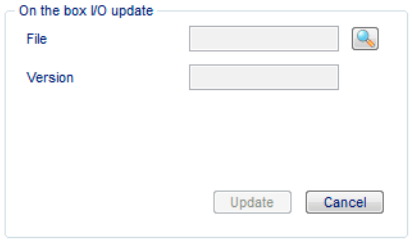
With an ENTRY system license you can install only 1 Main I/O card. Multiple Main I/O cards are not supported. Also, an ENTRY system does not support Extension I/O cards. This is for instance the case with the ADPRO RMG Lite.

3.4.1 Updating the Main I/O card

The current software version, loaded in the MIO card, is shown in the list.



To update the MIO card to a more recent software version, open **System > Connections > I/O**, select the desired MIO card and click **Update**. On the right a new section appears:



Locate the file “usbio.img” (with the latest software version) via the *magnifying glass* button.

The version of the selected file is shown. Click **Update** to load the new version in the MIO card.

3.4.2 USB I/O Address Range

3.4.2.1 Main I/O and Extension I/O: Set 1

I2560	I/O card absent	C2560	green LED*
		C2561	yellow LED*
		C2562	blue LED*
		C2563	buzzer*
I2576 / I2596	alarm / tamper on input 1	C2576	output 1
I2577 / I2597	alarm / tamper on input 2	C2577	output 2
I2578 / I2598	alarm / tamper on input 3	C2578	output 3
I2579 / I2599	alarm / tamper on input 4	C2579	output 4
I2580 / I2600	alarm / tamper on input 5	C2580	output 5
I2581 / I2601	alarm / tamper on input 6	C2581	output 6
I2582 / I2602	alarm / tamper on input 7	C2582	output 7
I2583 / I2603	alarm / tamper on input 8		
I2584 / I2604	alarm / tamper on input 9		
I2585 / I2605	alarm / tamper on input 10		
I2586 / I2606	alarm / tamper on input 11		
I2587 / I2607	alarm / tamper on input 12		
I2588 / I2608	alarm / tamper on input 13		
I2589 / I2609	alarm / tamper on input 14		
I2590 / I2610	alarm / tamper on input 15		
I2591 / I2611	alarm / tamper on input 16		

I2592 / I2612	alarm / tamper on input 17		
I2593 / I2613	alarm / tamper on input 18		
I2594 / I2614	alarm / tamper on input 19		
I2595 / I2615	alarm / tamper on input 20		

* Status of front LED indicators and buzzer.

3.4.2.2 Main I/O and Extension I/O: Set 2

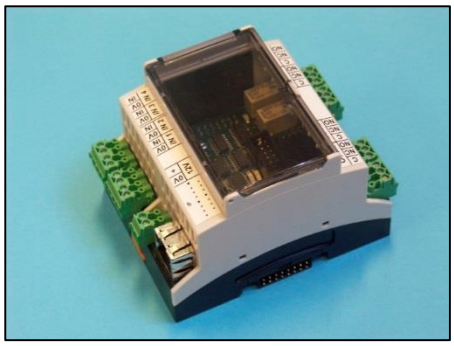
I2560	I/O card absent	C2624	green LED *
		C2625	yellow LED *
		C2626	blue LED *
		C2627	buzzer *
I2640 / I2660	alarm / tamper on input 1	C2640	output 1
I2641 / I2661	alarm / tamper on input 2	C2641	output 2
I2642 / I2662	alarm / tamper on input 3	C2642	output 3
I2643 / I2663	alarm / tamper on input 4	C2643	output 4
I2644 / I2664	alarm / tamper on input 5	C2644	output 5
I2645 / I2665	alarm / tamper on input 6	C2645	output 6
I2646 / I2666	alarm / tamper on input 7	C2646	output 7
I2647 / I2667	alarm / tamper on input 8	C2647	output 8
I2648 / I2668	alarm / tamper on input 9		
I2649 / I2669	alarm / tamper on input 10		
I2650 / I2670	alarm / tamper on input 11		
I2651 / I2671	alarm / tamper on input 12		
I2652 / I2672	alarm / tamper on input 13		
I2653 / I2673	alarm / tamper on input 14		
I2654 / I2674	alarm / tamper on input 15		
2655 / I2675	alarm / tamper on input 16		
I2656 / I2676	alarm / tamper on input 17		
I2657 / I2677	alarm / tamper on input 18		
I2658 / I2678	alarm / tamper on input 19		
I2659 / I2679	alarm / tamper on input 20		

* Front LED indicators and buzzer are always controlled by set 1.

3.5 Net I/O Modules

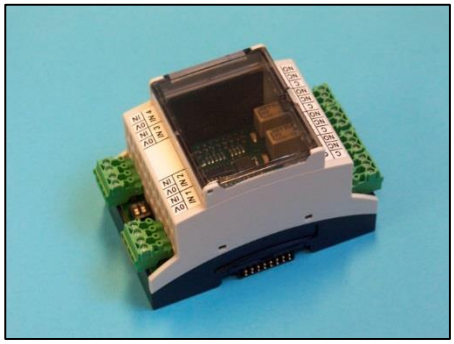
Please consult the technical data sheet on the ADPRO FastTrace 2 Ethernet Net I/O Module. You can download the data sheet from the Xtralis Support website www.xtralissecurity.com (logon required).

The RMG can be linked to up to 8 Network I/O modules. These modules – mounted on a DIN Rail installation – are connected to the local network, and powered by PoE or by a local adapter (12 VDC; 800 mA) or injector. Each I/O module receives a number from 1 to 8 when it is added to the list, and offers 4 inputs and 4 outputs.



Each I/O module can be extended with 1 to 3 submodules, to obtain up to 16 inputs and outputs.

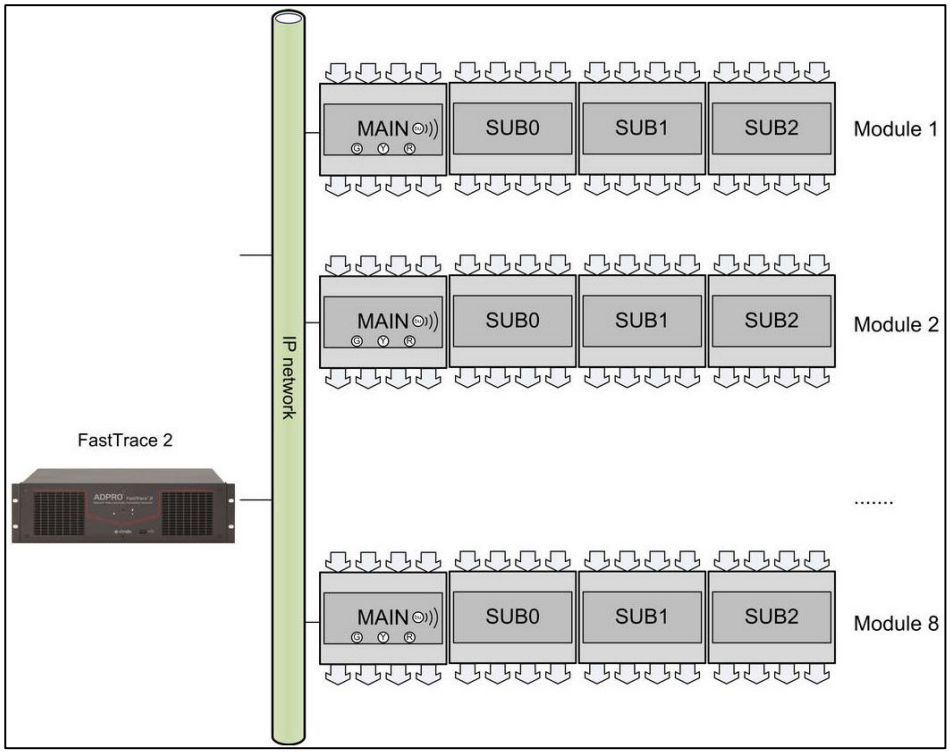
Network I/O modules also have LED indicators and a buzzer which are controlled by the RMG.



Network I/O modules return fault conditions on 4 separate addresses.

Faults include:

- module is starting up
- module has been reset
- module power fault
- module not present



3.5.1 Ordering Information

Please use these order numbers for the ADPRO FastTrace 2 Ethernet I/O modules:

Base unit	49841000
Extension unit	49841010

3.5.2 Net I/O Address Range

3.5.2.1 Inputs

Alarm	**Address**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	
1	I2050	I2114	I2178	I2242	I2306	I2370	I2434	I2498	Module Power Loss
2	I2051	I2115	I2179	I2243	I2307	I2371	I2435	I2499	Module Presence Fault

Digital input	**Address**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Module**
1	I2080	I2114	I2208	I2272	I2336	I2400	I2464	I2528	main
2	I2081	I2145	I2209	I2273	I2337	I2401	I2465	I2529	
3	I2082	I2146	I2210	I2274	I2338	I2402	I2466	I2530	
4	I2083	I2147	I2211	I2275	I2339	I2403	I2467	I2531	
5	I2084	I2148	I2212	I2276	I2340	I2404	I2468	I2532	sub0
6	I2085	I2149	I2213	I2277	I2341	I2405	I2469	I2533	
7	I2086	I2150	I2214	I2278	I2342	I2406	I2470	I2534	
8	I2087	I2151	12215	12279	12343	12407	12471	12535	
9	I2088	I2152	I2216	I2280	I2344	I2408	I2472	I2536	Sub1
10	I2089	I2153	I2217	I2281	I2345	I2409	I2473	I2537	
11	I2090	I2154	I2218	I2282	I2346	I2410	I2474	I2538	
12	I2091	I2155	I2219	I2283	I2347	I2411	I2475	I2539	
13	I2092	I2156	I2220	I2284	I2348	I2412	I2476	I2540	Sub2
14	I2093	I2157	I2221	I2285	I2349	I2413	I2477	I2541	
15	I2094	I2158	I2222	I2286	I2350	I2414	I2478	I2542	
16	I2095	I2159	I2223	I2287	I2351	I2415	I2479	I2543	

3.5.2.2 Outputs

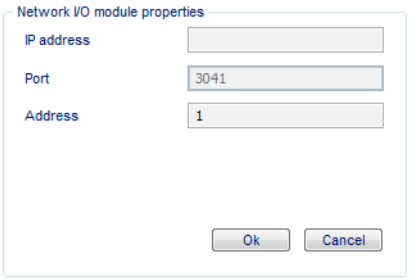
	Address								
Out	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	
0	C2048	C2112	C2176	C2240	C2304	C2368	C2432	C2496	Green LED
1	C2049	C2113	C2177	C2241	C2305	C2369	C2433	C2497	Yellow LED
2	C2050	C2114	C2178	C2242	C2306	C2370	C2434	C2498	Red LED
3	C2051	C2115	C2179	C2243	C2307	C2371	C2435	C2499	Buzzer

Relay output	Address								
	1	2	3	4	5	6	7	8	Module
1	C2080	C2144	C2208	C2272	C2336	C2400	C2464	C2528	main
2	C2081	C2145	C2209	C2273	C2337	C2401	C2465	C2529	
3	C2082	C2146	C2210	C2274	C2338	C2402	C2466	C2530	
4	C2083	C2147	C2211	C2275	C2339	C2403	C2467	C2531	
5	C2084	C2148	C2212	C2276	C2340	C2404	C2468	C2532	sub0
6	C2085	C2149	C2213	C2277	C2341	C2405	C2469	C2533	
7	C2086	C2150	C2214	C2278	C2342	C2406	C2470	C2534	
8	C2087	C2151	C2215	C2279	C2343	C2407	C2471	C2535	
9	C2088	C2152	C2216	C2280	C2344	C2408	C2472	C2536	Sub1
10	C2089	C2153	C2217	C2281	C2345	C2409	C2473	C2537	
11	C2090	C2154	C2218	C2282	C2346	C2410	C2474	C2538	
12	C2091	C2155	C2219	C2283	C2347	C2411	C2475	C2539	
13	C2092	C2156	C2220	C2284	C2348	C2412	C2476	C2540	Sub2
14	C2093	C2157	C2221	C2285	C2349	C2413	C2477	C2541	
15	C2094	C2158	C2222	C2286	C2350	C2414	C2478	C2542	
16	C2095	C2159	C2223	C2287	C2351	C2415	C2479	C2543	

3.5.3 Adding Net I/O Module with Known IP Address

Open the *I/O* window via System > Connections > I/O.

Click **Add**. On the right you will see the section *Network I/O module properties* appears.

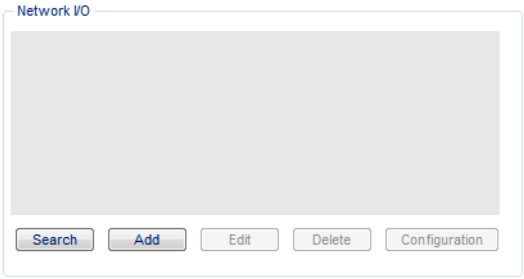


Enter IP address and address (= order number) of the Net I/O module (1–8). The port number (i.e. the port to which the I/O module is listening) cannot be modified.

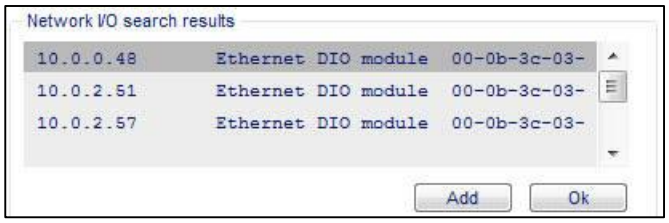
Click **OK** to add the I/O module. Click **Save** to save the modifications.

3.5.4 Searching Net I/O Modules on the Local Network

Open the *I/O* window via System > Connections > I/O.



Click **Search**. Underneath the section *Network I/O search results* will appear.

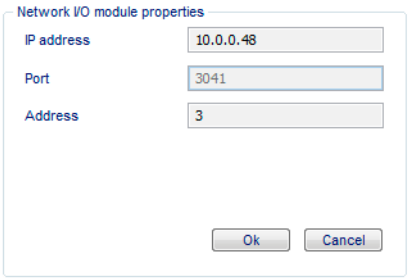


Select the desired I/O module and click **Add**. The selected Net I/O module is now shown in the list *Network I/O*.

Add all desired Net I/O modules and then click **OK**. In the list with Network I/O modules, select the desired module to edit and/or configure.

3.5.5 Modifying the IP Settings of a Net I/O Module

Open the *Net I/O configuration* window via **System > Connections > I/O**. Select the desired Net I/O module from the list and click **Edit**.



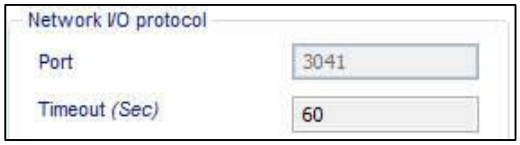
Enter the IP address and Net I/O address (order number 1–8). Click **OK** and **Save**.

3.5.6 Net I/O Module Inputs and Outputs Setup

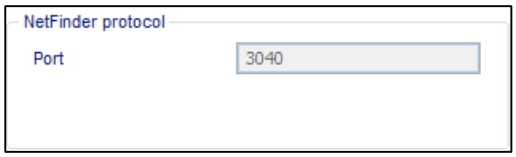
Open the *I/O* window via **System > Connections > I/O**. Select the desired Net I/O module from the list and click **Configuration**.

Modify the name of the network I/O module. It is recommended to use a meaningful and relevant description.

Modify the port of the Net I/O module. This port should be the same port as selected when the I/O module was added.

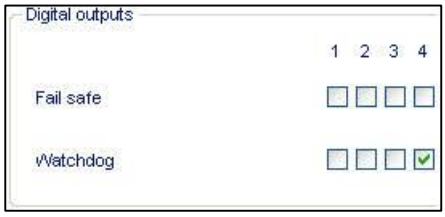


You cannot modify the port used by the Netfinder tool. Netfinder is an external tool used to program the IP address of an I/O module and to update its software. You can find this tool on the CD/DVD delivered with the system, or you can download it from the Xtralis Support website www.xtralissecurity.com.



Digital inputs may be inverted. Normally the input is configured as NO (normally open). If you tick the *Inverted* option, the input will be configured as NC (normally closed).

Digital outputs can be configured for failsafe operation and/or watchdog operation. Fail safe operation means that the relay is inverted: the output will be activated when idle. Watchdog operation means that the output will be activated on communication time-out (network I/O protocol time out, to be defined via **System > Behaviour > Alarm transmission > General**).



Click **Save**.

3.6 Connection to Presidium

You can associate video outputs from a Presidium with FastTrace 2 analogue inputs. Use coax cables to connect the video outputs of the Presidium system to the video inputs of a FastTrace 2 video system for further analysis and recording. It is then possible to transmit alarms from the Presidium to the RMG over the IP network.

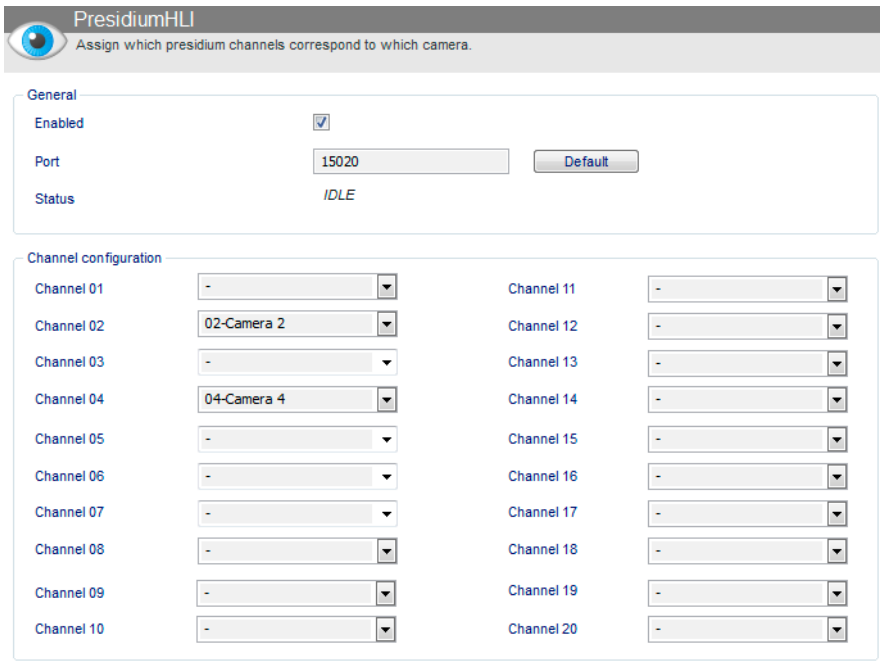
For hardware setup, see the *FastTrace 2 Hardware Installation Manual*.

The connection to a Presidium can trigger the following events on the RMG:

- I0070 – [SYST] – PRESIDIUM FAULT: the Presidium reports a high temperature or general fault, or the RMG detects an incorrect IP port.
- I0071 – [SYST] – PRESIDIUM PRES. FAULT: no communication with the Presidium.
- I1024 – [REAL] – CAM01: video signal is missing on camera 1 (detected by the Presidium).
- I1025 – [REAL] – CAM01 CONTRAST ERROR: camera 1 lens is covered (detected by the Presidium).
- I1033 – [REAL] – CAM01 PRESIDIUM DET: alarm on camera 1 (detected by the Presidium).

To set up the Presidium connection, proceed as follows:

1. Choose **System > Connections > PresidiumHLI**.
2. Select the **Enabled** check box.
3. In the **Port** box, type the IP port through which the Presidium can communicate with the server.
4. In the **Channel configuration** pane, assign the Presidium video outputs to the server inputs.



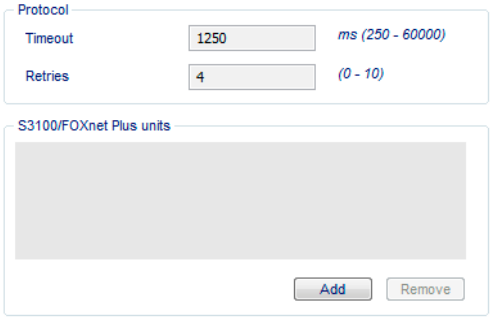
5. Click **Save**.

3.7 Connection to S3100

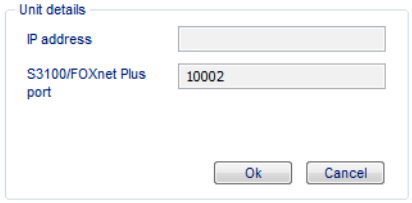
You can connect the server with the Xtralis S3100 system. You can add multiple S3100 security panels. Each S3100 security panel can activate one of the 8 available virtual inputs on the RMG video system. For more information, see the S3100 technical documentation. For more information on configuring the virtual inputs, see *Alarm Profiles* on page 97.

To set up the connection with an S3100 security panel, proceed as follows:

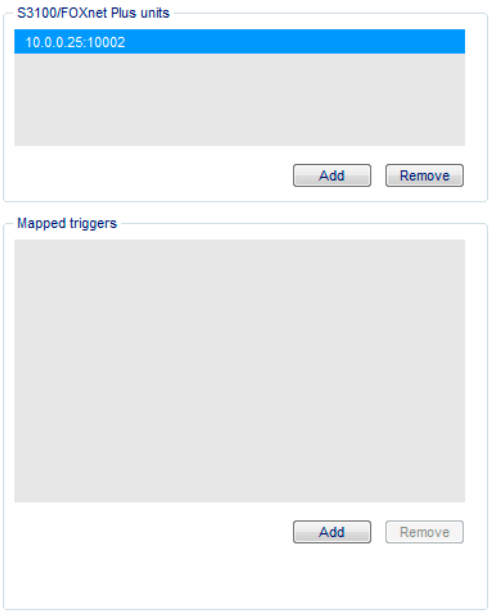
1. Choose **System > Connections > Video interconnection**.
2. Enter the desired protocols. The default values normally suffice, but can be increased on slower networks if you observe communication faults between the interconnected devices.



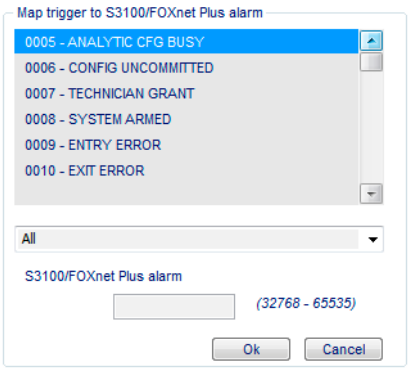
3. Click **Add**. The following panel appears:



4. In the **IP address** box, enter the IP address of the S3100 security panel.
5. In the **S3100/FOXnet Plus port** box, enter the port number for communication (as defined in the security panel).
6. Click **OK** to confirm.
7. Click the added S3100 security panel in the list, and then click **Add** in the **Mapped triggers** pane.



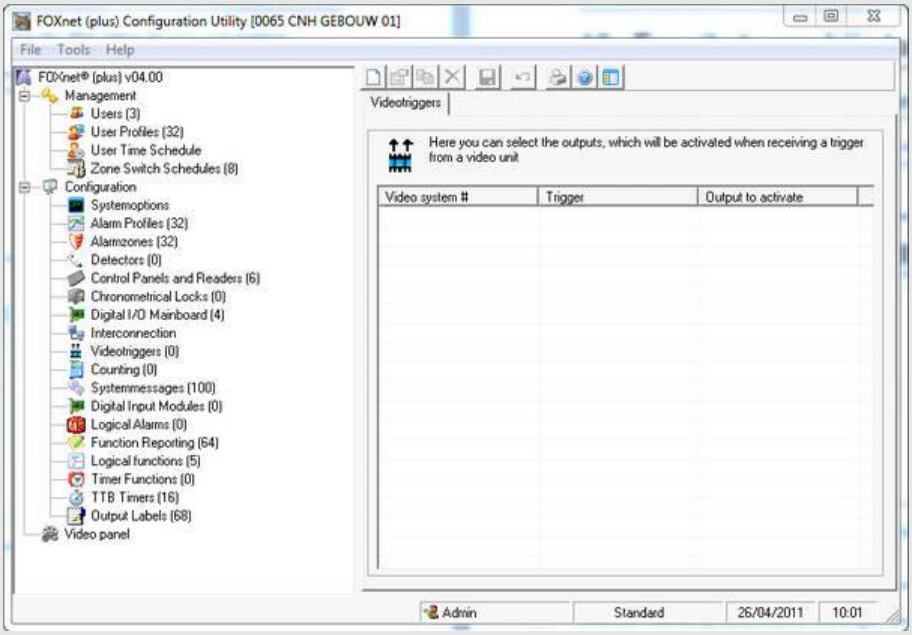
The following pane appears:

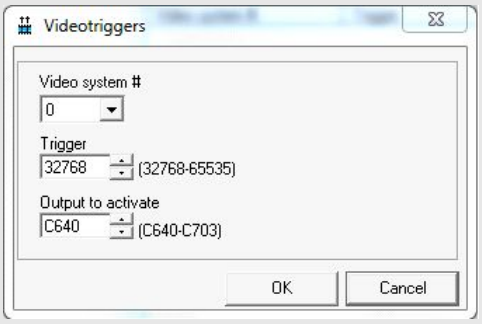


8. Select an alarm and associate the alarm to a trigger. Use the filter option for your convenience.
9. In the S3100 security panel, you need to associate the trigger with an output. This output will be activated when the system detects the associated event (e.g. hard disk error).
10. Click **Save**.

Note

In the S3100 Configurator, open *Video triggers* and click **New** to associate the selected trigger to the output.





Interconnection also works with the older FOXNet (Plus) security panels.

3.8 Email

3.8.1 Setting up Email

If you want the video system to send emails on events/alarms, set up the email SMTP server and email sender address. Ask the IT Department for the correct settings.

Note

The email address of the email sender may need to be an existing email account, depending on the SMTP server settings.

To set up email communication, proceed as follows:

1. Choose **System > Connections > Email**.

2. Provide the **SMTP server address**, **SMTP server port**, **TLS**, **Username** and **Password** as specified by the IT Department.
3. In the **Sender email address** box, type the email address that will send the emails.
4. For emails to the iTrace app, specify the following additional settings:
   - **iTrace smtp retry time (1–10m)**: specify the time (between 1 and 10 minutes) in which the recipient must respond to the iTrace email. If the recipient does not respond in time, iTrace sends the email again.
   - **iTrace retry attempts (1–10)**: the number of times (between 1 and 10) that iTrace sends an email for the same event. If there is still no response from the recipient after that, RMG generates the system message NO ITRACE REACTION (I0041). This message can warn CMS staff that there was no response to the iTrace emails, so that they can then take the appropriate action.
5. Click **Save**.

You can now set up the mailing lists to send emails to.

3.8.2 Creating Mailing Lists

The email address book defines the email addresses for sending alarm messages. For each trigger, or set of triggers, you can create a mailing list that contains the email addresses of everyone who needs to be informed of the alarm or event.

You can indicate that the mailing list is for specific use with iTrace. The emails then have a different layout, so that iTrace can display the correct alarm information.

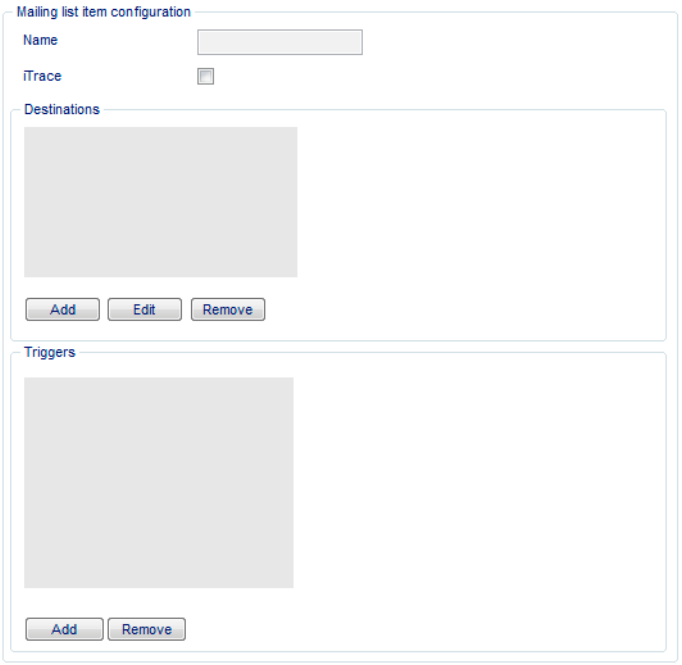
> ***Caution!***
>
> Make sure that you link all the triggers used for emails to alarm profiles with **Email transmission** enabled. For example, you cannot use triggers with alarm profile SILENT MESSAGE, because **Email transmission** is disabled for silent messages. If necessary, create a separate alarm profile.

To create a mailing list, proceed as follows:

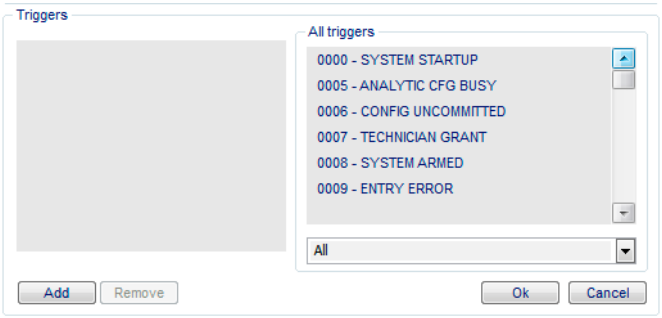
1. Choose **System > Behaviour > Email Addressbook**.

E-Mail Addressbook
Define here what people will get an e-mail when certain alarms are generated. You can define which camera pictures will be attached for these alarms in the 'Input/Output Behaviour' page.
Mailing list
Add
Edit
Remove

2. Click **Add**. The following screen appears:

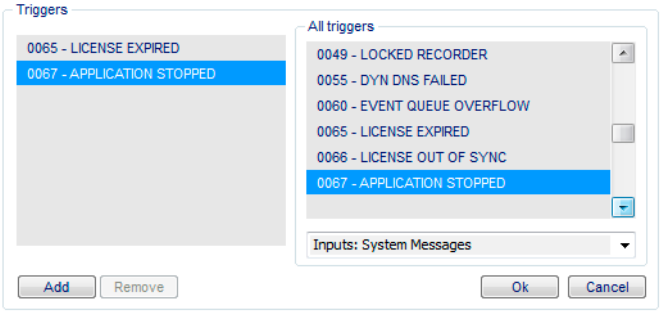


3. In the **Name** box, type a meaningful name for the mailing list.
4. If the mailing list is used with iTrace iCommand, select the **iTrace** check box.
   First, you will add the required email addresses.
5. Under **Destinations**, click **Add**.
6. In the **Email address** box that appears, type the email address, and then click **OK**.
7. Repeat for all other required destination addresses.
8. To remove an email address, click on the address, and then click **Remove**.
9. To change an email address, click on the address, and then click **Edit**. Change the email address as required and then click **OK** to confirm.
   Now you can add the inputs that will trigger the email.
10. Under **Triggers**, click **Add**. The list with all possible triggers appears.



Use the filter below the list to reduce the list.

11. To add a trigger, double-click it in the **All triggers** list. The selected trigger now appears in the **Triggers** box:



12. To remove a trigger from the **Triggers** list, double-click it.

13. Click **OK** to save the triggers.
14. Click **OK** to save the mailing list.
15. Click **Save** to save the email address book.

3.8.3 Verifying Email Communication

From firmware version V2.11, the server sends a test/confirmation email when you save the changes in the email address book. Check if the recipient has received this test/confirmation email.
If not, revise the settings for the email connection and the email address book.

All versions prior to V2.11 do not send this email, so please verify correct operation as mentioned below.

Verify correct operation of the email notification as follows:

1. Select your mailing in the **Mailing list** box, and then click **Edit**.
2. In the **Triggers** box, add any event that you can easily trigger (such as connection to the unit or an input).
3. Click **OK**, and then click **Save** to save the changes.
4. Trigger the event.
5. Check if the recipient receives a notification email. If not, revise the settings for the email connection and the email address book.
6. If yes, remove the test event from the **Triggers** box.
7. Click **OK** to save the triggers.
8. Click **OK**, and then click **Save**.

4 Using IP Cameras

Please check the *Supported IP Cameras* list before connecting IP cameras to the server. You can download the list from the Xtralis Support website www.xtralissecurity.com.

4.1 RMG Units with HIPI Card (FastTrace 2 Series Only)

When your FastTrace 2 RMG unit is equipped with one or two HIPI cards, you do not need to take any action to activate the IP camera channels. One HIPI card automatically provides 8 IP camera channels. The camera setup screen displays the number of remaining IP camera channels (see *IP Camera Setup* on page 51).

4.2 RMG Units with IP Gateway Card (FastTrace 2 Series Only)

The FastTrace 2E RMG units are equipped with an IP gateway card. When using the IP gateway card, you have to activate IP channel licenses. These licenses are provided as application licenses in sets of 4 (providing either 4, 8, 12, 16, or 20 IP channels). You deploy them on your FastTrace 2E unit via the Xtralis Xchange Tool. You can always purchase extra sets of IP application licenses to add to your FastTrace 2E unit.

The camera setup screen displays the number of remaining IP camera channels (see *IP Camera Setup* on page 51).

Note

It is not allowed to use both HIPI cards and IP gateway cards in one FastTrace 2 unit. When the FastTrace 2 unit detects a HIPI card, it will automatically use the HIPI card and ignore any IP licenses!

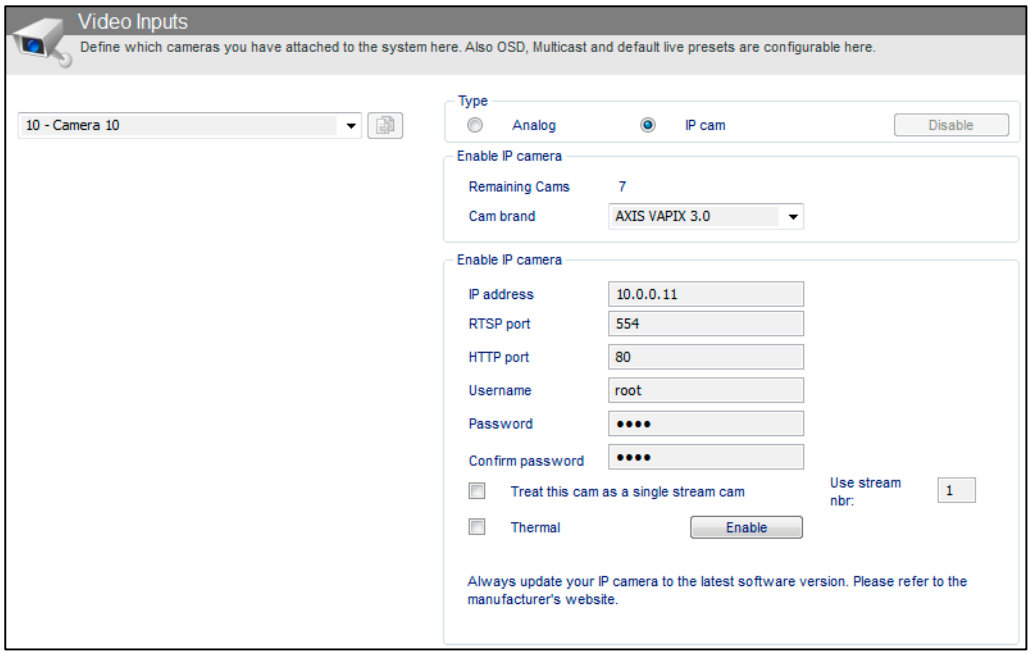
4.3 IP Camera Setup

Note

You need to configure the HIPI/Ethernet card(s) before configuring the IP cameras. For more information, see *IP Camera Network Configuration* on page 32.

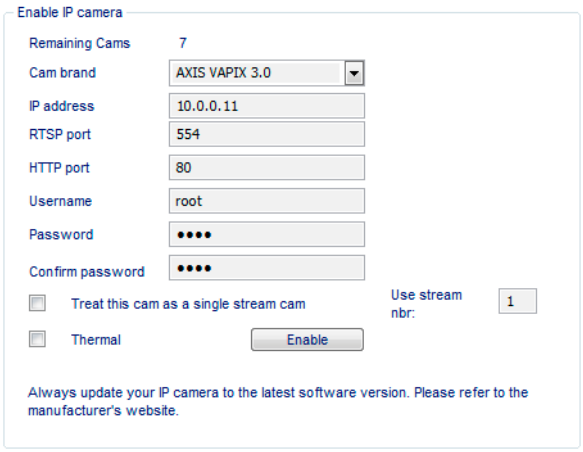
To add an IP camera, you need to connect the camera to the network and open **System > Connections > Video inputs**. Then choose a free camera number from the list.

Under **Type**, click **IP cam**.


Video Inputs
Define which cameras you have attached to the system here. Also OSD, Multicast and default live presets are configurable here.
10 - Camera 10
Type
Analog
IP cam
Disable
Enable IP camera
Remaining Cams 7
Cam brand AXIS VAPIX 3.0
Enable IP camera
IP address 10.0.0.11
RTSP port 554
HTTP port 80
Username root
Password ••••
Confirm password ••••
Treat this cam as a single stream cam
Use stream nbr: 1
Thermal
Enable
Always update your IP camera to the latest software version. Please refer to the manufacturer's website.

The **Remaining Cams** box displays the number of remaining IP camera channels.

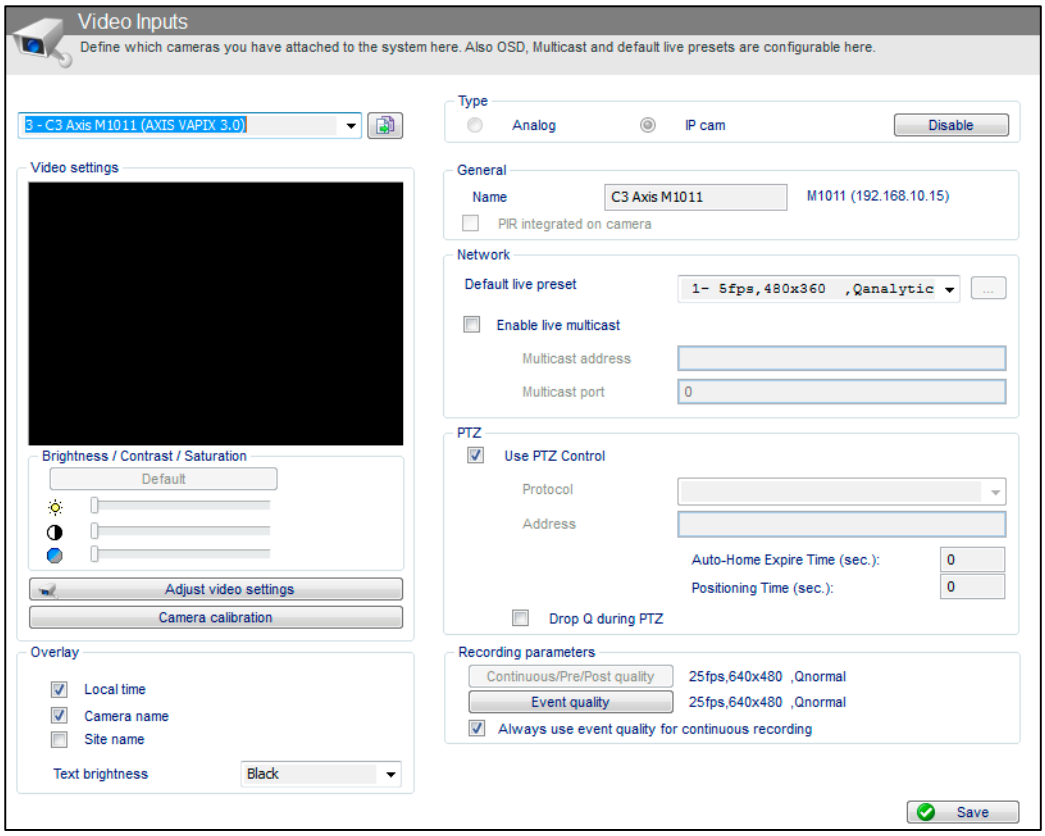
Select the camera brand and type the correct IP address, the username and corresponding password of the camera (e.g. “root” for Axis cameras). Check the camera documentation for the correct password.


Enable IP camera
Remaining Cams 7
Cam brand AXIS VAPIX 3.0
IP address 10.0.0.11
RTSP port 554
HTTP port 80
Username root
Password ••••
Confirm password ••••
Treat this cam as a single stream cam
Use stream nbr: 1
Thermal
Enable
Always update your IP camera to the latest software version. Please refer to the manufacturer's website.

If you tick the option **Treat this cam as a single stream cam**, only one stream will be used for all features related to the server. This means, however, that there will be specific limitations in the RMG video system: the only stream that the RMG video system will use is the analytics stream. As a result this will be a CIF resolution at 5 fps (or the minimal quality available on the camera). Typically, the analytics stream from a camera is stream 1. However, if the camera uses a different stream for analytics, you can specify the stream number in the **Use stream nbr** box.

If you tick the option *Thermal* the camera will be enabled as thermal camera.

Click **Enable** to start using the IP camera.

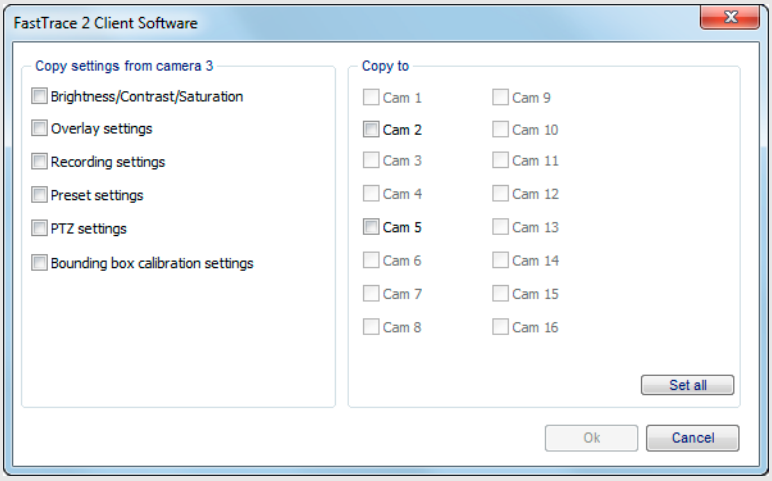


Then complete the necessary parameters.

Note

You can copy the settings of one camera and paste these to another camera. Use the **Copy** button next to the camera list.

You will get the following popup window:



4.3.1 General Parameters

Name	Enter a description for the camera (max 20 characters). It is recommended to use a meaningful and relevant description.

PIR integrated on camera	Check this option when a PIR has been integrated on this camera. The option is only available if the IP camera has an integrated PIR (e.g. Axis M1054). Activating this integrated PIR will enable you to send/receive PIR alarms for this specific camera.

4.3.2 Video Settings

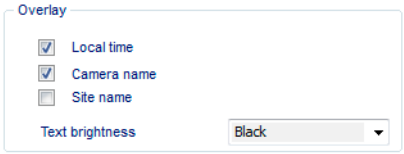
You need to click **Adjust video settings** to be able to make any modifications. From the moment you activate this, you will obtain the live image from the IP camera.

4.3.3 Brightness/Contrast/Saturation

If the image does not provide enough quality, you can adjust brightness, contrast, and hue in the *Brightness / Contrast / Saturation* section.

4.3.4 Overlay

Local time	Tick this option if you want to display the local time on the camera's live image.
Camera name	Tick this option if you want to display the camera name on the camera's live image.
Site name	Tick this option if you want to display the site name on the camera's live image.
Text brightness	This option is not available for IP cameras. The parameter can be added to the IP camera settings via the camera's web browser.



4.3.5 Network

Default live preset	When watching live images from a camera, the image quality can be adjusted at any time by clicking your right mouse button. The initial quality, applied the first time you select the camera, can be specified with this parameter. You can choose from different preset qualities, depending on the camera. If you choose "Hard disk stream", live pictures will follow the same quality as continuous recordings. This way, only two streams are required.
...	With certain types of IP cameras this button becomes active. Via this button you can open the list with possible quality presets. The parameters you can modify here, are: • Frames per second (fps) • Resolution of the picture • Quality: VBR quality (Qlow, Qnormal or Qhigh) or CBR bit rate (20 through 2048 kbps). The higher the value, the better the quality, but also the higher the bandwidth use! Remark: for stable image quality, VBR is recommended.

Only live multicast	Multicast is the simultaneous supply of information to one or more computers through only one data stream from the source. When multiple computers poll this one stream, multiple copies will be created, but the initial upload will remain the same. Multicast thus ensures less data traffic over the network. The 224.0.0.0 through 239.255.255.255 address range has been assigned for multicasting on the local LAN network. Tick this option if you want to use the multicast protocol.
Multicast address	Enter the address to which the RMG video system has to send the multicast. ***Note*** Every camera should be assigned to a unique multicast address. Everyone who has subscribed to the multicast, can view the live images on this address, using a web browser or an XOa client.
Multicast port	Enter the multicast port through which the RMG has to send the stream.

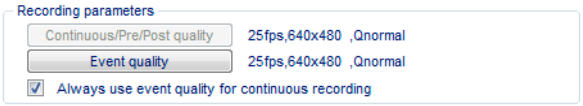
4.3.6 PTZ

Use PTZ Control	Tick this option if you have installed a PTZ camera.
Protocol	Choose the corresponding protocol for the IP camera you have installed.
Address	Enter the correct camera address for the IP camera you have installed. Check the camera settings to know the camera address.
Auto-Home Expire Time (sec)	This value indicates the time in seconds that has to expire after every PTZ action, before the PTZ camera will move back to its home position. If the value is left to 0, the Auto-Home feature will be disabled.
Positioning Time (sec.)	PTZ preset positions can be selected via an input. When that input triggers the PTZ action, the camera will move to the configured PTZ preset position, but the alarm message of the input will be delayed until the PTZ preset positioning time has expired. Thus no blurry images are recorded for quad images.
Drop Q during PTZ	Select this option if you want to drop the image quality during PTZ movements.

Note

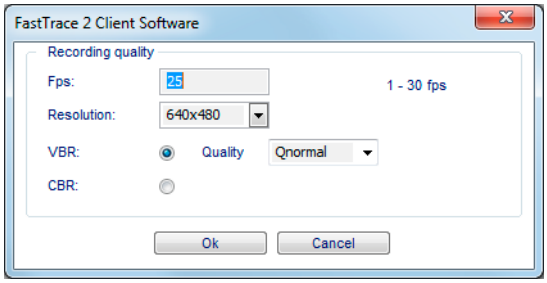
When the *Auto-Home Expire Time* has been configured, the analytics detection will be suppressed during PTZ movement. Only when the camera has returned to the home position, the analytics detection will resume.

4.3.7 Recording



Continuous/Pre/Post quality	This shows the quality that has been configured for continuous recordings and for pre and post event recording.
Event quality	This shows the quality that has been configured for the event recording.
Always use event quality for continuous recording	When you activate this option the quality settings for continuous recording will be changed to the event quality settings (and no longer use the analytics quality setting).

Set the recording parameters by clicking the desired quality.



- Fps: the number of frames per second (1–25);
- Resolution: the number of pixels per image; depends on the camera type;
- VBR: selects a variable bitrate compression (Qlow, Qnormal or Qhigh);
- CBR: selects a constant bitrate compression (value 20–2048 kbps*); the higher the value, the lower the compression, the higher the quality and the higher the consumed bandwidth. The video quality level is constantly adapted to fulfil the required bitrate setting. VBR with Qnormal quality is recommended!

* This range is for analogue inputs and may differ for IP cameras.

Click **Save**.

Note

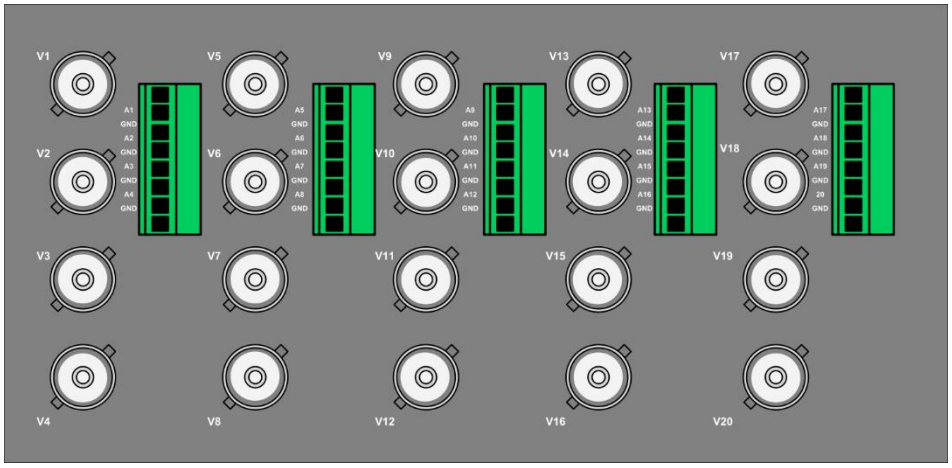
Before using the IP camera, you need to set up a static IP address in the camera, create a password for the user “root”, and set the date and time. You can adjust the time and date manually or you can synchronize the camera in the RMG to an NTP protocol.

Check the manual provided with the camera for more information on setting up the IP address, password, and clock.

5 Using Analogue Cameras

5.1 Video and Audio Connections

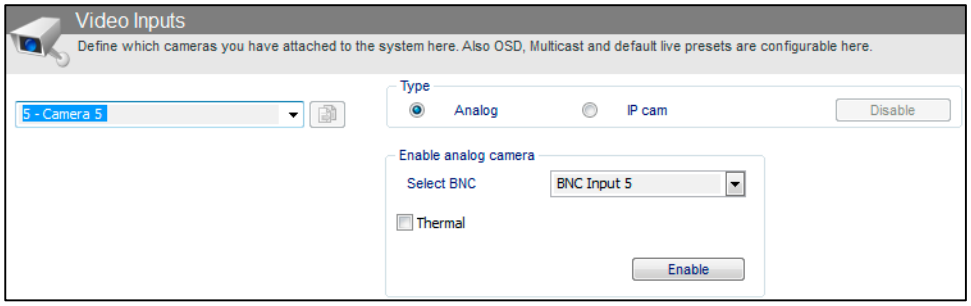
Analogue cameras can be connected to the rear of the RMG video system using a BNC connecting RG59 or RG11 cable.



Each camera needs a separate BNC input! Depending on the configuration of your server, you will have 4, 8, 12, 16, or 20 analogue BNC camera inputs.

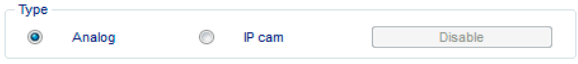
5.2 Analogue Camera Setup

To add an analogue camera, you need to connect the camera to the video system and open **System > Connections > Video inputs**. Then choose a free camera number from the list:

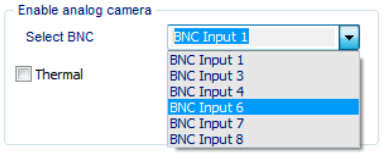


Up to 20 cameras can be connected to the RMG video system. For every analogue camera 1 A/V input is required.

Tick the *Analog* option:



Select the BNC input and click **Enable**.

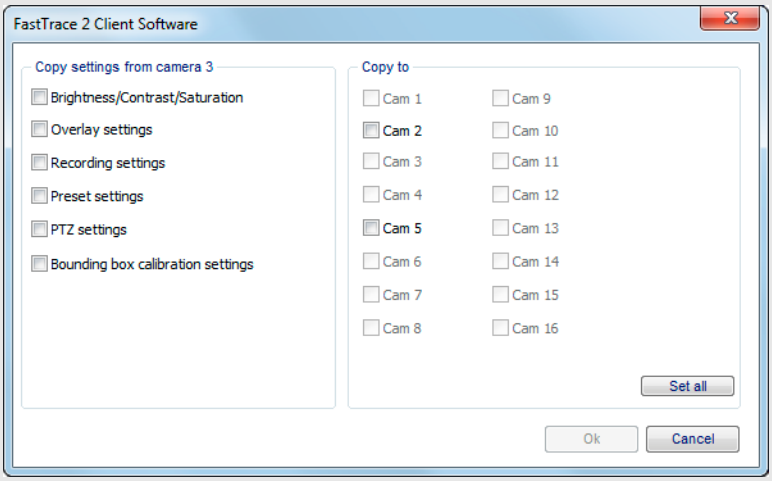


When enabled you can adjust some parameters.

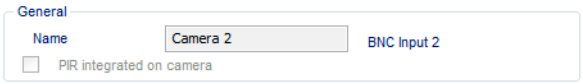
Note

You can copy the settings of one camera and paste these to another camera. Use the **Copy** button next to the camera list.

You will get the following popup window:



5.2.1 General Parameters



In the **Name** box, type a meaningful and relevant name for the camera (max. 20 characters).

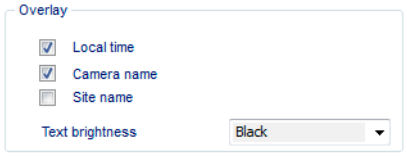
5.2.2 Video Settings

You need to click **Adjust video settings** to be able to make any modifications. From the moment you activate this, you will obtain the live image from the analogue camera.

5.2.3 Brightness/Contrast/Saturation

If the image does not provide enough quality, you can adjust brightness, contrast, and hue in the *Brightness / Contrast / Saturation* section.

5.2.4 Overlay



Local time	Tick this option if you want to display the local time on the camera's live image.
Camera name	Tick this option if you want to display the camera name on the camera's live image.
Site name	Tick this option if you want to display the site name on the camera's live image.
Text brightness	Choose the colour of the text that is displayed on the image.

5.2.5 Network

Default live preset	When watching live images from a camera, the image quality can be adjusted at any time by clicking your right mouse button. The initial quality, applied the first time you select the camera, can be specified with this parameter. You can choose from different preset qualities, depending on the camera. If you choose “Hard disk stream”, live pictures will follow the same quality as continuous recordings. This way, only two streams are required.
	With certain types of cameras this button becomes active. Via this button you can open the list with possible quality presets. The parameters you can modify here, are: • Frames per second (fps) • Resolution of the picture • Quality: VBR quality (Qlow, Qnormal of Qhigh) or CBR bit rate (20 through 2048 kbps). The higher the value, the better the quality, but also the higher the bandwidth use! ***Note*** For stable image quality VBR is recommended.
Only live multicast	Multicast is the simultaneous supply of information to one or more computers through only one data stream from the source. When multiple computers poll this one stream, multiple copies will be created, but the initial upload will remain the same. Multicast thus ensures less data traffic over the network. The 224.0.0.0 through 239.255.255.255 address range has been assigned for multicasting on the local LAN network. Tick this option if you want to use the multicast protocol.
Multicast address	Enter the address to which the RMG video system has to send the multicast. ***Note*** Assign a unique multicast address to each camera. Everyone who has subscribed to the multicast, can view the live images on this address, using a web browser or an XOa client.
Multicast port	Enter the multicast port through which the RMG has to send the stream. ***Note*** Assign a unique multicast port to each camera. The IT Department must define the port before connecting the RMG.

5.2.6 PTZ

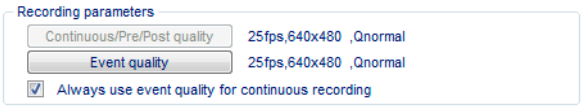
Use PTZ Control	Tick this option if you have installed a PTZ camera.
Protocol	Choose the corresponding protocol for the camera you have installed.
Address	Enter the correct camera address for the camera you have installed. Check the camera settings to know the camera address.
Auto-Home Expire Time (sec)	This value indicates the time in seconds that has to be expired after every PTZ action, before the PTZ camera will move back to its home position. If the value is left to 0, the Auto-Home feature will be disabled.

Positioning Time (sec.)	PTZ preset positions can be selected via an input. When that input triggers the PTZ action, the camera will move to the configured PTZ preset position, but the alarm message of the input will be delayed until the PTZ preset positioning time has expired. Thus no blurry images are recorded for quad images.

Note

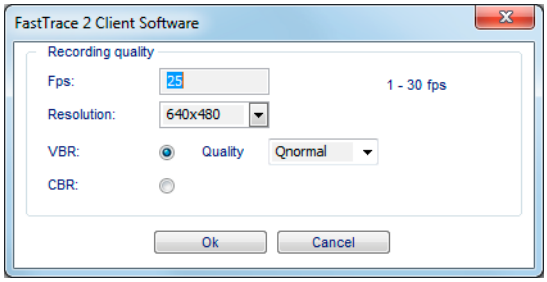
When the Auto-Home Expire Time has been configured, the analytics detection will be suppressed during PTZ movement. Only when the camera has returned to the home position, the analytics detection will resume.

5.2.7 Recording



Continuous/Pre/Post quality	This shows the quality that has been configured for continuous recordings and for pre and post event recording.
Event quality	This shows the quality that has been configured for the event recording.

Set the recording parameters by clicking the desired quality.



Fps	The number of frames per second (1–25)
Resolution	The number of pixels per image; depends on the camera type
VBR	Selects a variable bitrate compression (Qlow, Qnormal or Qhigh)
CBR	Selects a compressed bitrate compression (value 20–2048 kbps); the higher the value, the higher the compression and the lower the loss of quality; the compression levels will differ according to the constant data flux in which the file size is predictable, but the quality will depend on the video contents.

VBR with Qnormal quality is recommended!

Click **Save**.

5.3 List of Available PTZ Protocols

The server supports the following PTZ protocols:

- 360 Vision / Vantage Juno / VT Fastrax-P / Xeno Neodome
- Amux IEC
- Baxall ZMX
- Baxall ZTX
- BBV
- Burle/Philips/Bosch
- COHU
- Pacom
- Panasonic (conventional)
- Panasonic (new)
- Pelco D
- Pelco D (no zoom speed)
- Pelco P
- Samsung
- Sensormatic

- Conway
- CS Lilin
- CS Lilin 2
- Dennard 2050
- Diamond
- Digital Sprite
- Elbex
- Ernitec
- GPS
- Grundig
- Harris
- JVC
- Kalatel
- Mark Mercer
- Molynx
- Molynx Variable Speed
- Sensormatic Controller
- Sensormatic Speeddome VII
- Siemens
- Synectics
- TEB
- TEB (rail)
- Unidex
- VCL
- Vicon
- Video Switch
- Visca
- Vista Powerdome

Note

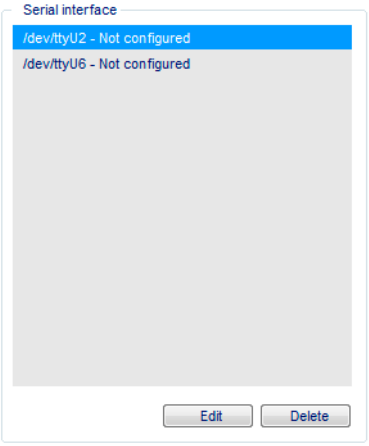
- When using the Pelco Spectra Cam 4, the PTZ address has an offset of -1 in the XOa client.
- When using the JVC protocol, the PTZ address has an offset of +1 in the XOa client.

Example:
When using a JVC protocol with address 1 in the XOa client, the PTZ address of the camera is 2.

5.4 PTZ Control via USB Port/MIO Card

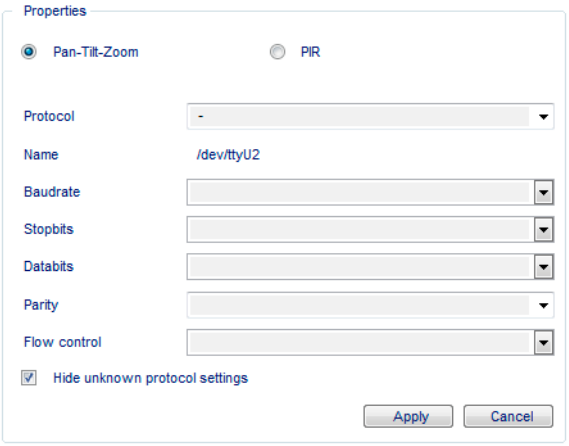
To set up the connection for PTZ control via USB port or MIO card, proceed as follows:

1. Choose **System > Connections > Serial Ports / PTZ**.



2. Select the correct port in the list:
   - For a connection via the first MIO card, select **/dev/ttyU6**.
   - For a connection via the second MIO card, select **/dev/ttyU8**.
   - For a connection via USB, consult the *FastTrace 2 Hardware Installation Manual* for the correct port number.

3. Click **Edit**.



4. Choose the correct option: **Pan-Tilt-Zoom**.
5. Select the desired protocol, depending on the camera type. Enter baud rate, stop bits, data bits, parity, and flow control according to the camera specifications. Normally the settings are correct when choosing the protocol. Clear the **Hide unknown protocol settings** check box if you want to modify the default settings.
6. Click **Apply** and **Save** to maintain any modifications.

Note

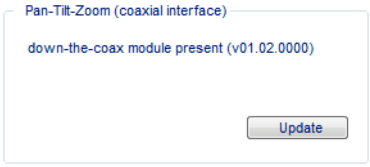
The external USB ports, used for PTZ control, can be found at the rear of the server. A converter to convert USB to RS-232 or RS-485 is required.

Note

Telemetry station manufacturers provide a variety of models and features. The server provides PTZ control ability for a number of popular models and where possible, supports the features provided by the manufacturer. Due to the number of models available on the commercial market, details of connection and use for individual models have not been provided in this manual. Xtralis does, however, have tech tips available for these cameras on the Xtralis Support website www.xtralissecurity.com.

5.5 PTZ Control via DTC Card

Open the PTZ window via **System > Connections > Serial Ports / PTZ**. Check if the DTC card is present.



Note

The current software version loaded in the DTC card is shown in the list. To update the DTC card to a more recent software version, open **System > Connections > Serial Ports / PTZ**. Click **Update** and locate the file *dtc.img* with the latest software. Click **Apply**.

These PTZ protocols are supported on the DTC card:

- Down-the-Coax (Pelco Ext.)
- Down-the-Coax (Baxall Std.)
- Down-the-Coax (Baxall Alt.)
- Down-the-Coax (BBV coax)

6 Recording Mode Schedule

6.1 Operational Modes

The video system can operate in up to 4 different modes. In each mode, the video recorder can behave differently. For example, you can record continuously in one mode, and record only on events in another mode. There are several ways to switch from one operational mode to another:

- Automatically, according to a time schedule. See *Operational Mode with Time Schedule* on page 63.
- Manually, using an input as a switch. See *Operational Mode with Manual Selection* on page 64.
- It is also possible to change the operational mode using third-party software. For more information, see the documentation of the ADPRO XOa Software Development Kit (SDK).

The sections below describe how to set up automatic or manual switching.

To define the input that you want use as a switch, see *Input/Output Behaviour* on page 107.

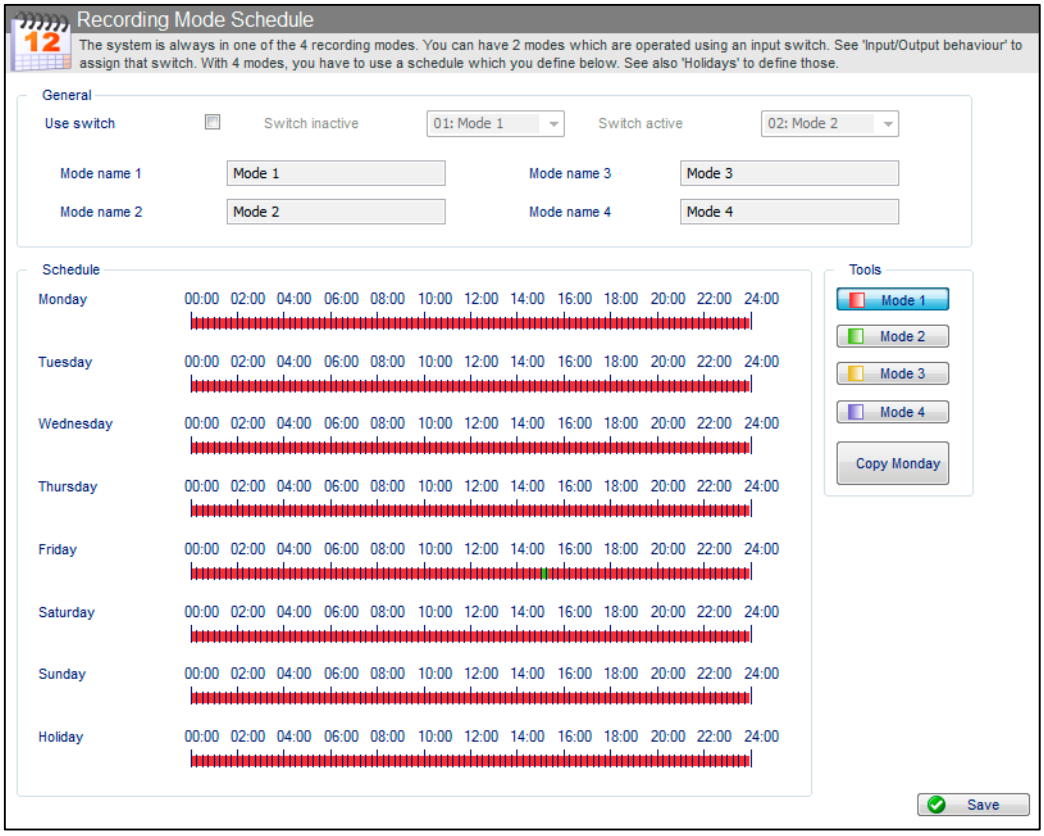
To define how the video recorder behaves in each mode, see *Recordings Behaviour* on page 66.

6.2 Operational Mode with Time Schedule

With a time schedule, you can automatically switch between up to 4 operational modes. You define which mode is active when. Only one mode can be active simultaneously.

To set up automatic switching between operational modes, proceed as follows:

1. Choose **System > Behaviour > Recording Mode Schedule**.

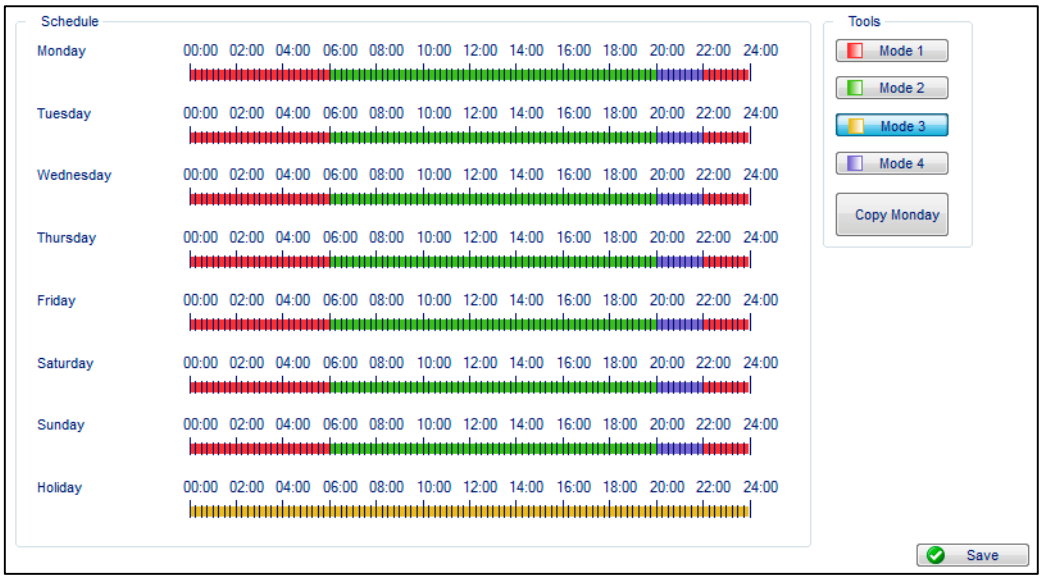


2. Make sure that the **Use switch** check box is cleared.
3. In the **Mode name 1** to **Mode name 4** boxes, type a meaningful name for each of the operational modes. You can use up to 20 characters. An example:
   - Mode 1 = DAY
   - Mode 2 = NIGHT
   - Mode 3 = HOLIDAY

- Mode 4 = EMERGENCY

The **Schedule** pane shows a time bar for each day, and one for holidays. By default, the system operates in mode 1 during the whole schedule: all time bars are red.

4. Under **Tools**, click the desired mode button (**Mode 1**–**Mode 4**) and then drag the mouse over the day and time when the mode has to be active. Where you drag, the time bar changes to the colour of the selected mode.
5. If you have a repeating schedule, you can copy the schedule from Monday to all other days (including holidays): click **Copy Monday**, and then click **Yes** to confirm.
6. Adjust until you have the correct schedule for each day.



7. Click **Save**.

The system now switches automatically from one mode to another according to the schedule.

6.3 Operational Mode with Manual Selection

If you use manual selection, you can switch between two operating modes. You define the modes, and the input that serves as a switch.

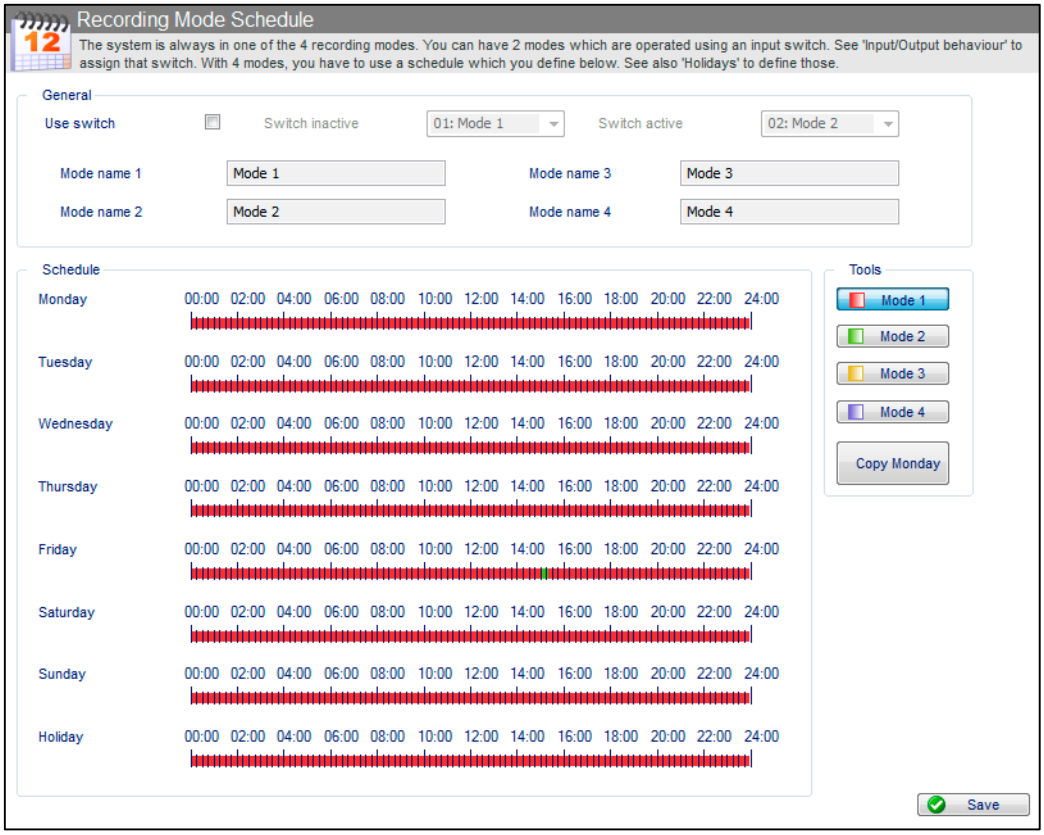
To define an input as operational mode switch, see *Input/Output Behaviour* on page 107.

Note

If you use manual selection (switch), you can use only two operational modes. If you need more modes, then you have to use the time schedule instead of the switch.

To set up manual switching between two operational modes, proceed as follows:

1. Choose **System > Behaviour > Recording Mode Schedule**.



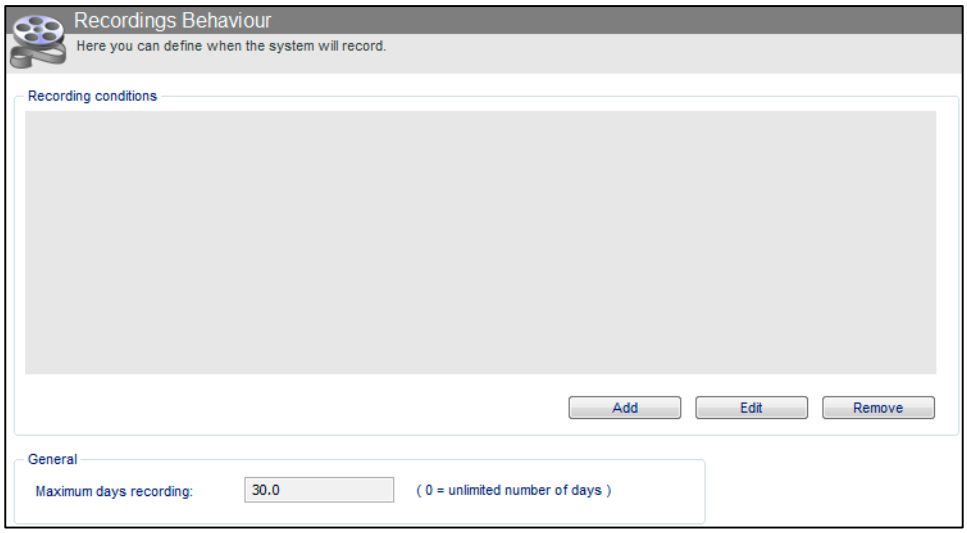
2. Select the **Use switch** check box.
3. In the **Switch inactive** box, select the operational mode that you want to use when the switch is inactive.
4. In the **Switch active** box, select the operational mode that you want to use when the switch is active.
5. In the **Mode name** boxes for the two selected modes, type a meaningful name for the modes. You can use up to 20 characters. An example:
   - Mode 1 = DAY
   - Mode 2 = NIGHT
6. Click **Save**.

The system now switches from one mode to another according to the input.

7 Recordings Behaviour

7.1 Setting up Recordings

Open the *Recordings Behaviour* window via **System > Behaviour > Recordings Behaviour**.

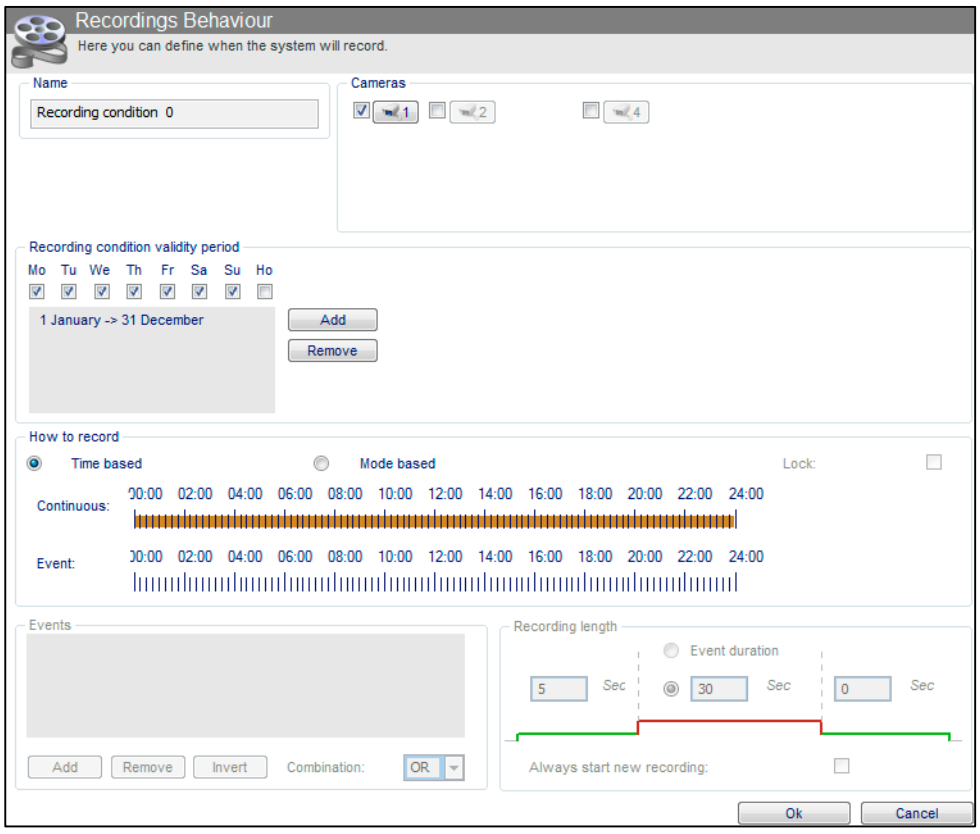


To add a new recording, click **Add**.

To edit an existing recording, select the recording in the list and click **Edit**.

To delete an existing recording, select the recording in the list and click **Remove**.

If you add a new recording or edit an existing recording, the specific settings of the recording can be entered:



7.1.1 Name

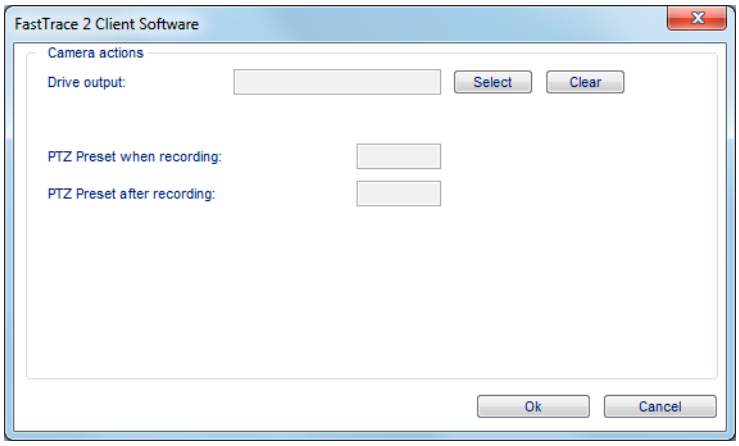
By default the name *Recording condition 0* (or any next number depending on the number of recording conditions that have been defined) is provided. It is recommended to change the name into a meaningful and relevant description. A maximum of 20 characters can be used.

7.1.2 Cameras

Tick the desired camera. You can tick multiple cameras if necessary.

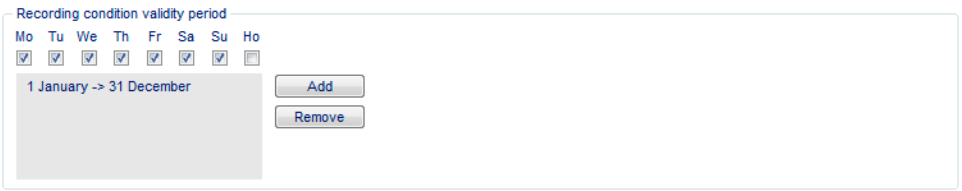
Click the camera number to:

- activate an output when recording (you need to set up a recording-controlled output first, see *Input/Output Behaviour* on page 107);
- go to a preset position (PTZ) when the recording is started;
- go to a preset position (PTZ) when the recording is ended.



Click **OK** to save and apply any modifications you might have made and return to the previous window.

Next, tick the days on which the specific recording should be made. The recording is by default active during the full year. If you want this recording to apply only for limited periods, delete the listed period and add a customized period.



Select the **Ho** check box to enable recording on holidays (see *Calendar* on page 133).

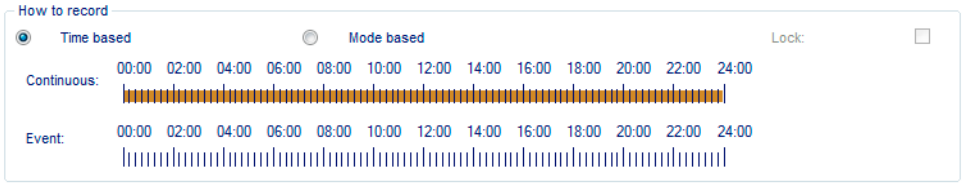
You can add multiple periods in which the recording should be active.

Next, you can specify when exactly the recording has to take place.

7.2 Continuous Recording

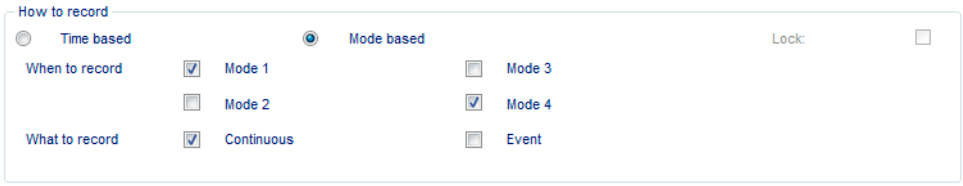
Select **Time based** to activate the recording in function of a time schedule. Click and hold the left mouse button and drag the mouse over the ***Continuous*** time scale to mark the time zone during which the recording should be active. To correct for errors, right-click the time scale to clear the time zone and retry.

Up to 8 time zones can be defined.



Select **Mode based** to activate the recording in function of the operational mode of the video system. The operational mode (1 to 4) is programmed automatically (with mode schedule) or manually (with switch).

For more information on switching modes, see *Recording Mode Schedule* on page 63.



Tick **Continuous** for What to record.

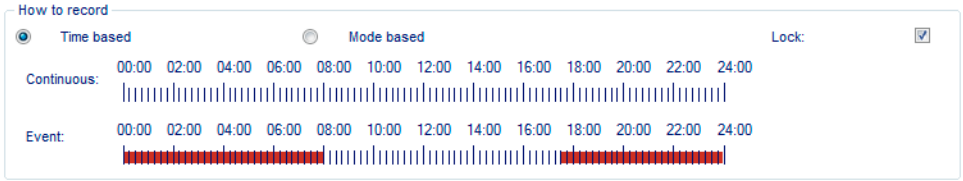
Click **OK** and **Save** to apply the new settings.

> ***Note***
>
> Continuous recording is not allowed with a Transmission-only system license.

7.3 Recording on Event

Select "**Time based**" to activate the recording in function of a time schedule. Click and hold the left mouse button and drag the mouse over the ***Event*** time scale to mark the time zone during which the recording should be active. To correct for errors, right-click the time scale to clear the time zone and retry. To prevent any conflicts, it is recommended to clear the ***Continuous*** time scale.

Up to 8 time zones can be defined.

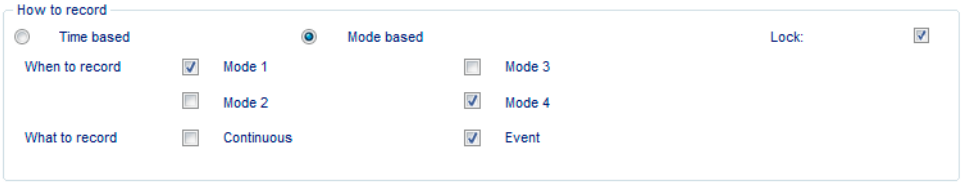


On recording on event it is also possible to "lock" the recording. This means that the recording cannot be erased automatically. Furthermore, locked recordings trigger the system message 0049 – [SYST] – LOCKED RECORDER (by default linked to the alarm profile NORMAL EVENT).

> ***Caution!***
>
> XOa cannot delete locked recordings. When it encounters a locked recording during automatic clean-up (for example after 30 days), RMG stops cleaning up and **also stops recording**. For more information on handling locked recordings, see *Locked Recordings* on page 90.

Select "**Mode based**" to activate the recording in function of the operational mode of the video system. The operational mode (1–4) is programmed automatically (with mode schedule) or manually (with switch).

See also *Operational Mode with Time Schedule* on page 63.



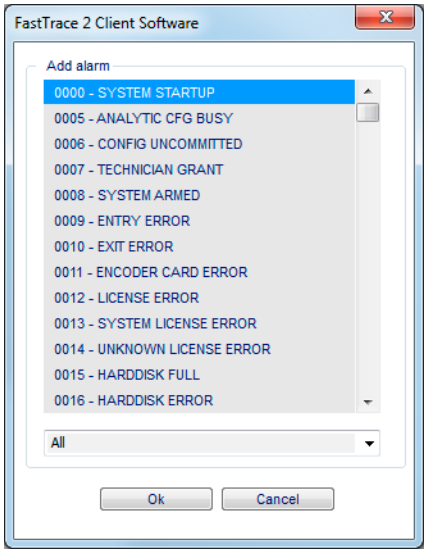
Tick **Event** for What to record.

Click **OK** and **Save** to apply the new settings.

> ***Note***
>
> You could also tick the Continuous mode for “What to record” to create a mixed recording. Such recording will record continuously at the chosen quality and will switch to another quality on the selected event(s).

In the section *Events* click **Add**.

The following window appears:



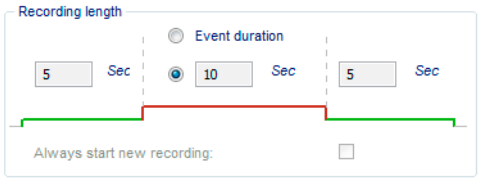
Select the desired alarm trigger and click **OK**.

Several conditions can be added. For each condition you should define whether the condition should also be fulfilled (AND) or whether this condition alone should trigger the alarm (OR). You cannot combine AND an OR conditions.

If you invert the alarm, the recording will start when the end-of-alarm is received.

In the section *Recording length* you can define the duration of the recording. It is possible to set a time (value in seconds) for recording before, during, and after the event. For recording during the event you have the choice between *Event duration* or a predefined period.

When the triggers follow each other so quickly that the recordings overlap, the multiple recordings will be melted into 1 recording.



Click **OK** and **Save** to apply the new settings.

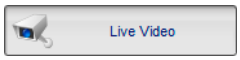
Note

- If recordings with different quality settings overlap, the highest quality and image rate will be applied.
- The video system is limited to 16 000 events a day. If more events occur on the same day (overflow), the video system will automatically switch to continuous recording for all cameras. This will be seen on the time scale as blue bars. All these recordings will have CIF resolution, 25 ips and quality 75 (level of compression).
- With the TRANSMITTER system license the recording on event is fixed to 5 seconds on pre-recording, 10 seconds on event recording, and no post-recording.

8 Watching Live Images

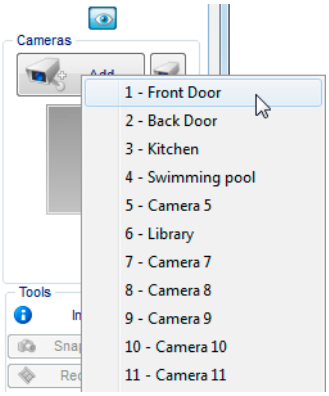
8.1 Watching Live Images in the Live Video Screen

Click **Live Video** to watch live video streams.

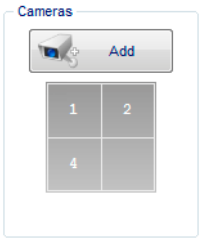


Select one or multiple cameras in the *Cameras* section.

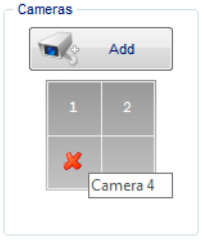
Click the **Add** button to obtain the available cameras to visualize:



Click the desired camera to visualize. The selected cameras are shown in the grey square in the *Cameras* section:



To delete a specific camera from the visualisation, click the delete button that appears when you place your mouse over the camera grid in the menu:



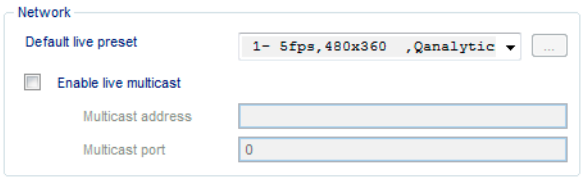
To close all live streams (remove all camera images from the **Live Video** screen), click the button.

When selecting only 1 camera, the window is fully taken by this camera's live stream.

When selecting multiple cameras, several camera streams will be visualized. The layout is rearranged automatically, to make sure all images are equally large. If you select 2 to 4 cameras, the display will automatically adjust to "quad" (= 4 images). With 5 to 9 cameras selected, you will automatically get 9 images, and so on.

You can double-click (with the left mouse button) one of the images to get a full screen view of the specific image. Double-click it again to see all the images.

The default quality of the image (resolution) has been defined in the video settings. Open **System > Connections > Video inputs** and select the desired video quality.



To adjust the quality of the image temporarily in the **Live Video** screen, right-click the camera image and select one of the options.

The available options depend on the type of camera.

If you want to see the bounding boxes of the analytics in your image, activate it by clicking the eye at the top of the menu on the right.

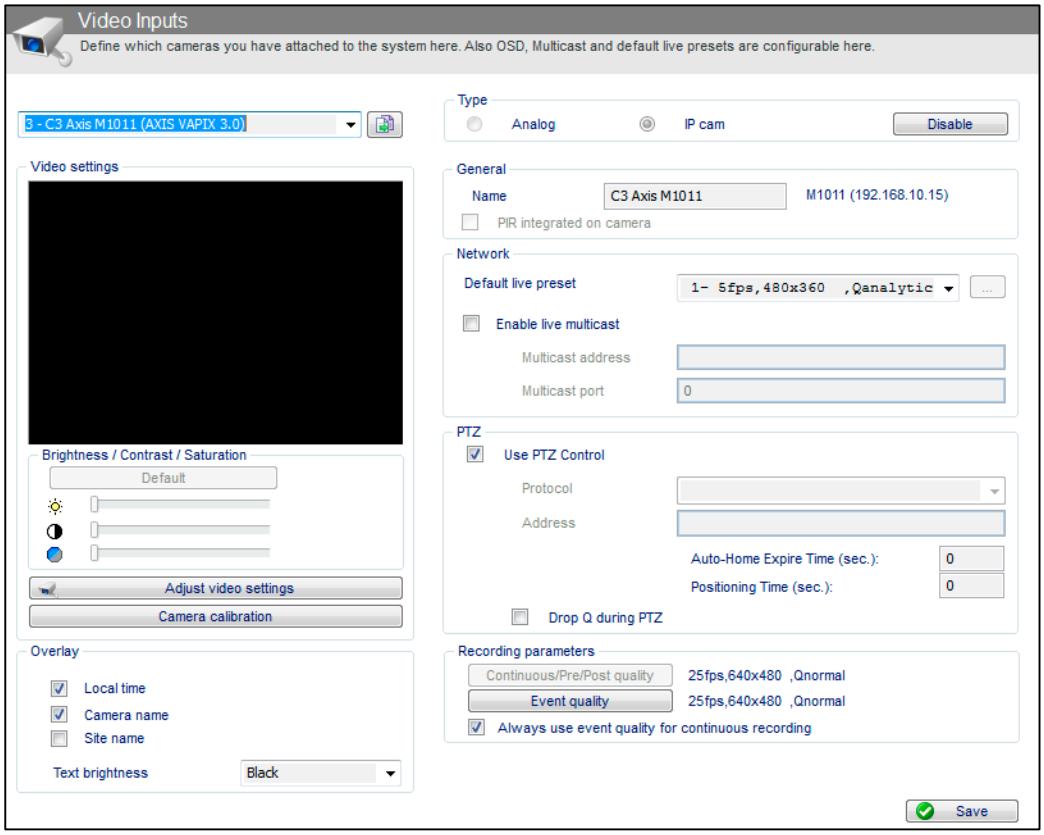
8.1.1 Live Video Streaming Limitations

For DS40xx A/V cards there is one separate video processor for each group of 4 analogue cameras (video in 1–4, 5–8, 9–12, and 13–16). If 4CIF resolution is applied to at least one camera within the same group, the following limitations apply to live streaming within this group of cameras (due to processor limits):

Number of enabled cameras within the same group	Live video resolution
1–2	no limits
3	only QCIF or CIF (25 ips); or the same quality as recording (hard disk stream)
4	only QCIF (25 ips); or the same quality as recording (hard disk stream)

For DS42xx A/V cards, the limitations are set per camera (and no longer per camera group). If recording quality is set to 4CIF/4SIF, the maximum quality for live viewing is CIF/SIF or QCIF/QSIF. When 2CIF/2SIF is applied for recording, only CIF/SIF, QCIF/QSIF and 2CIF/2SIF are possible with live viewing. Each time the maximum fps (frames per second) equals 25. All other combinations are of course possible.

Live streaming quality is defined under **System > Connections > Video Inputs > Network: Default live preset**.



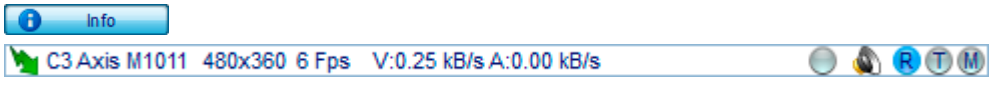
To set 4CIF/4SIF as default live preset, you need to set the recording quality to 4CIF/4SIF first, and then select hard disk stream as default live preset.

8.1.2 Tools

To the right you can find the section *Tools*. Here you can start/stop a manual recording and/or take a snapshot image of a specified live stream view.

8.1.2.1 Info Display

Click **Info** in the section *Tools* to visualise the information of the camera:



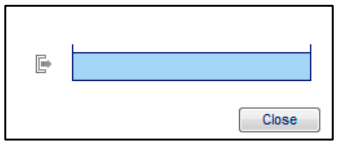
Legend:

	Video streaming status: • = connection OK • = connection error. The video image displays NO VIDEO. • = free live stream slot, no camera is assigned.
C3 Axis M1011	Camera name
480x360	Resolution

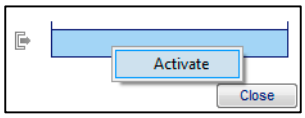
6 Fps	Number of frames per second
V:0.25 kB/s	Video stream transfer speed in kilobyte per second
A:0.00 kB/s	Audio stream transfer speed in kilobyte per second
	Local video recording (on hard disk of your PC): • blue = recording locally • grey = not recording locally
	Audio recording: • red = recording audio • grey = not recording audio If no audio is available, the loudspeaker icon is crossed out:
	Video recording (on the hard disk of the video system): • blue = recording • grey = not recording
	Tamper alarm. A contrast or sabotage event occurred on the camera. • yellow = tamper alarm active • grey = no tamper alarm
	Motion detection • green = motion detected • grey = no motion detected

8.1.2.2 Activating Outputs

You can activate outputs on the camera (if you have configured such outputs in **Input/Output Behaviour**). Click the button. (The button is only available if you have configured outputs.) A popup screen appears:



Right-click the output bar and click **Activate**.



Click **Close** to close the popup window.

8.1.2.3 Taking a Snapshot

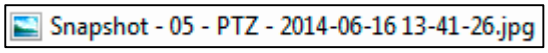
Via the buttons **Snapshot*** and **All** you can take a snapshot image of the video streams that are being shown at that specific moment.

These snapshots can be stored as images (jpg format) on your local hard disk (or a network folder you can access from your PC). You can also directly print the snapshots.

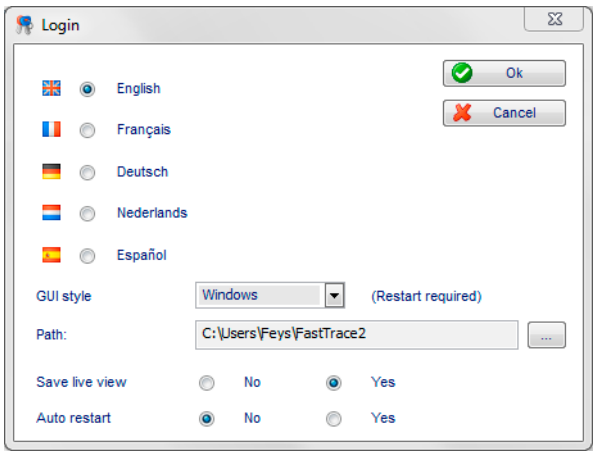
	Use these arrows to navigate to the different snapshots that have been taken.
	Save the snapshot that is shown to a folder on your local hard disk or a network folder.
	Save all snapshots to a folder on your local hard disk or a network folder.
	Print the snapshot that is shown to a printer of your choice.
	Print all snapshots to a printer of your choice.

* The option **Snapshot** should only be used when one of the camera images has been selected. If you select an image (= click the image in the live view with the left mouse button), a red border will appear around that image.

The snapshot file names contain the camera number and the time of taking the snapshot in the format year-month-day hours-minutes-seconds.

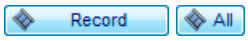


By default the work folder is selected to store the snapshot images. If you want to change the work folder, click **Settings** in the login window:



8.1.2.4 Local Video Recordings

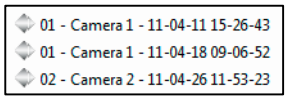
With the buttons **Record** and **All** you can store recordings locally (on the hard disk of your PC or a network folder).



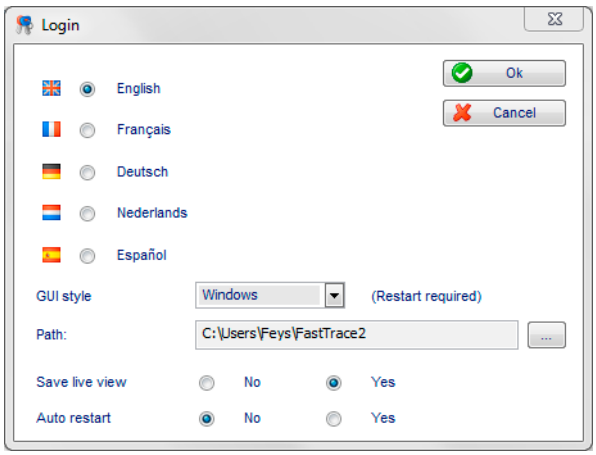
Click the button to start the recording. When a camera is recording locally, you can see a blue ball in the info section:

Click the same button to stop the recording.

The video recording file names contain the camera number and the time of recording in the format *year-month-day hour-minutes-seconds*. The files are stored with the extension .hbox.



By default the work folder is selected to store the snapshot images. If you want to change the work folder, click **Settings** in the login window:



8.1.3 Audio

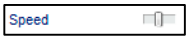
Select a camera. If it is a camera that supports audio (see *Audio IN* on page 35), you can activate the audio.

Click the loudspeaker to listen. The volume can be regulated through the slider. Click and hold the left mouse button on the slider and move the mouse to the desired level.

You can also talk to people if a microphone has been connected. Click and hold the left mouse button on the microphone. Also the volume of the microphone can be adjusted through the slider.

8.1.4 PTZ Control

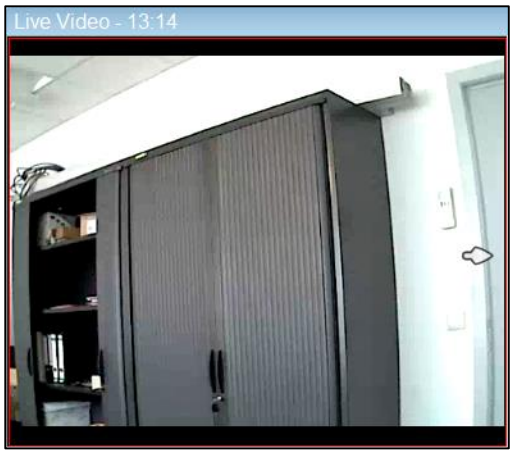
In the *PTZ* section you can control the PTZ cameras.

	Use the arrows to move the camera to the left or right and up or down. Use the “Home button” in the middle to move the camera to the selected preset position (= start position).
	When this button is lit (orange arrows), you can use digital zoom. Simply select a camera and you will see that the mouse indicator changes. Click the left mouse button and hold it to zoom in. To zoom out press the Shift key and the left mouse button. When zoomed in, the text **Digital Zoom** appears (in green letters) on the image.
	This slider adjusts the moving speed of the PTZ camera when using the player’s built-in controls.
	With this function you can zoom in or zoom out on a selected image.
	Click the middle button to manually adjust the focussing. Use the + and – buttons to adjust.
	Click to manually adjust the iris. Use the + and – buttons to adjust.
	Click to wash and/or wipe the lens of the outdoor camera. The camera has to have this feature of course.
	Store the camera position. Open the drop-down list to select one of the 4 possible camera preset positions. Click the floppy disk button to store the actual camera position in the selected preset number. Click the waste bin button to remove the preset position from the list.
	Enable or disable the selected auxiliary function on the camera. Auxiliary camera functions vary depending on the camera model. Please read the ADPRO Tech Tips for more information about auxiliary camera functions.

PTZ shortcut keys on the keyboard:

- Arrow keys (up, down, left, right)
- Home = Zoom in
- Page Up = Zoom out;
- End = Focus near;
- Page down = Focus far;
- Shift = Shift key enabled (only applies to new PTZ control).

Also on screen PTZ is available. Move your cursor to the edge of the image and it will transform in a white arrow. Keep the left mouse button pressed to go to a new position.



Note

Telemetry station manufacturers provide a variety of models and features. The RMG provides PTZ control ability for a number of popular models and where possible, supports the features provided by the manufacturer. Due to the number of models available on the commercial market, details of connection and use for individual models have not been provided in this manual. Xtralis does, however, have tech tips available for these cameras on the Xtralis Support website www.xtralissecurity.com.

8.2 Watching Live Images on a Monitor

8.2.1 About Using a Monitor

You can connect a monitor to the server, and use it for:

- Live viewing in a matrix view
- Consulting basic system information in the welcome screen
- Accessing the Installer menu for advanced hardware setup. For more information, see the *FastTrace 2 Hardware Installation Manual*.

If you use a monitor for live viewing instead of **Live Video**, the following restrictions apply:

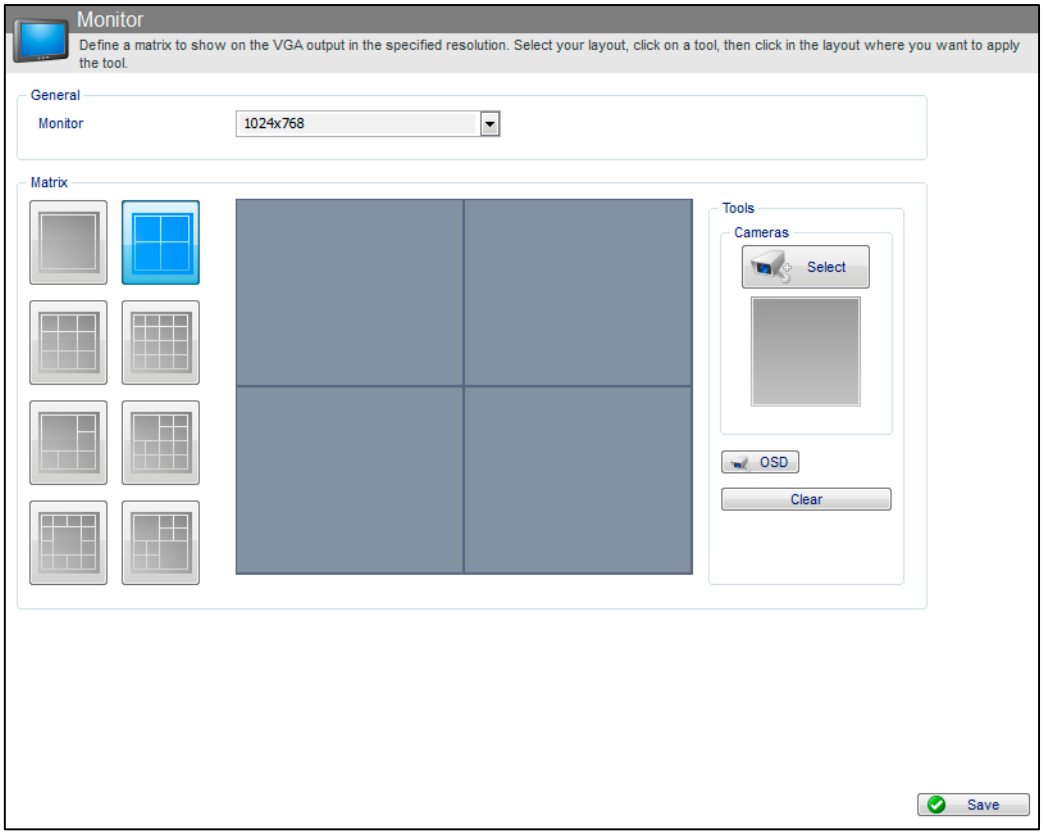
- You can view maximum 16 camera images.
- The image resolution is limited to CIF/SIF with Qnormal quality (analytics stream) at 5 fps.
- You cannot display analytics bounding boxes.
- The controls (tools, audio, PTZ) are not available.

8.2.2 Setting up a Monitor

To set up a monitor for live viewing, proceed as follows:

1. Choose **System > Connections > Monitor**.

2. In the **Monitor** box, select the desired resolution.



3. In the **Matrix** pane, click the desired matrix layout.
4. Add camera images to the matrix as follows: click **Select**, and click the desired camera in the popup list. Next, click the matrix cell where you want the camera image to appear.

> ***Note***
>
> You can assign a camera image to only one matrix cell.

5. To replace the existing camera image in a matrix cell, click **Select**, select a different camera, and then click the matrix cell.
6. To add the camera name on the matrix cell, click **OSD**, and then click each matrix cell where you want the camera name to appear. The camera name appears in the top left corner of the matrix cell. Click again to remove the camera name.
7. To remove camera images from the matrix, proceed as follows:
   - To remove one camera image, right-click the matrix cell.
   - To remove all camera images, click **Clear**.
8. Click **Save**.

8.2.3 Disabling the Matrix View

To disable the monitor matrix view, proceed as follows:

1. Choose **System > Connections > Monitor**.
2. In the **Monitor** box, select **Disabled**.
3. Click **Save**.

8.2.4 Switching Between Matrix View and Welcome Screen

You can easily switch between the matrix view and the welcome screen if you have a keyboard attached to the server:

- To switch to the welcome screen, press Ctrl+Alt+F1.
- To switch to the matrix view, press Ctrl+Alt+F7.

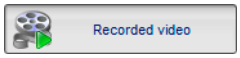
```
ADPRO XOa 03.00.0005
Ip     : 10.0.0.10
Subnet : 255.255.255.0
Gateway: 10.0.0.1

Port [HTTP]: 80
Port [CTRL]: 2000
Port [RTSP]: 554
```

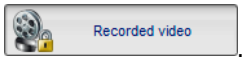
The welcome screen displays the following information:

- Server software version
- IP address, subnet mask, and gateway
- Http, control, and rtsp ports.

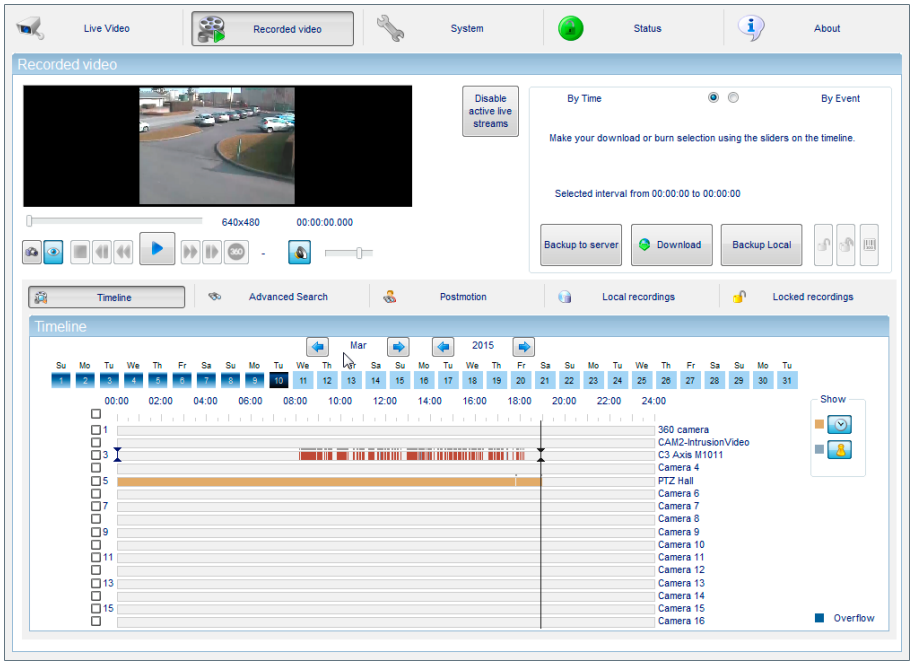
9 Searching Recordings and Watching Events

Open Recorded video.



If there are locked recordings on the system, a padlock appears on the button: 

. For more information on locking recordings, see *Recording on Event* on page 68.



9.1 Searching Recordings on the Timeline

Click Timeline.

9.1.1 Types of Video Recordings

Different types are recording are possible on the server. The colour on the timeline indicates the type of recording. You can choose to display or hide specific recording types on the timeline.

	Continuous recordings. Click the button in the **Show** panel to show/hide these recordings on the timeline.
	Recordings on event. This includes recordings from analytics such as LoiterTrace and IntrusionTrace. Click the button in the **Show** panel to show/hide these recordings on the timeline.
	Overlapping recordings: when triggers follow each other very quickly, recordings can overlap. This is indicated in purple bars on the timeline. You cannot hide overlapping recordings.
	Overflowing recordings: the server can record maximum 16 000 events per day (counter is reset at night). If more events occur on the same day (= overflow), the server switches automatically to continuous recording for all cameras. This is indicated in blue bars on the timeline. You cannot hide overflowing recordings.

When you change the recording types to show/hide on the timeline, playback stops. Click to resume playback.

Hover your mouse over a recording in the timeline to see its details:

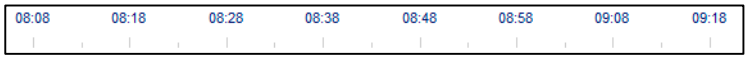
- Start and end time
- Event time
- Triggers that activated the event (not for continuous recordings).

9.1.2 Searching on the Timeline

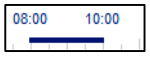
Choose the desired period (month and year) by using the arrow buttons.

Select the desired day. Only days that light up in dark blue contain recordings. The darkest day is the selected day.

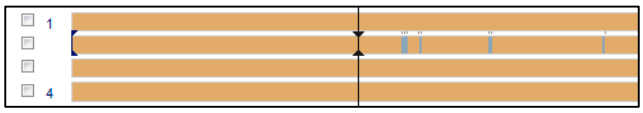
By default the time indication is shown with a 30 minutes interval. You can, however, zoom in on the time by dragging the mouse pointer (with the left mouse button pressed) on the time indication line. A blue marker appears to indicate the selected time.



When you stop pressing the left mouse button, the system will zoom in on the desired period of time.

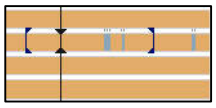


Select the timeline of the desired camera by clicking on that timeline with the left mouse button. A black arrow appears.



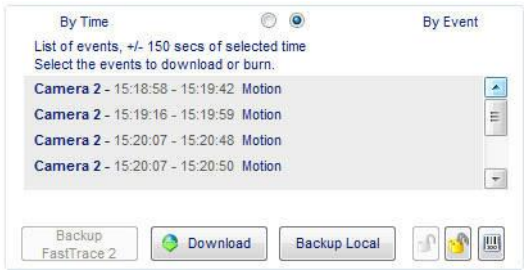
At the top left a still image of the selected camera is shown. Reposition the black arrow to choose another time. The image at the top left is adapted to the new time indication.

You can also reposition the black delimiters on the selected timeline. In doing this you set the start and end time of the video footage. It is the footage within this time frame that can be watched or downloaded.



9.1.3 Searching Recordings of Events

At the top right select the option “By event”. You will be shown a list of available recordings. The list contains only event recordings, no continuous recordings.


By Time
By Event
List of events, +/- 150 secs of selected time
Select the events to download or burn.
Camera 2 - 15:18:58 - 15:19:42 Motion
Camera 2 - 15:19:16 - 15:19:59 Motion
Camera 2 - 15:20:07 - 15:20:48 Motion
Camera 2 - 15:20:07 - 15:20:50 Motion
Backup FastTrace 2
Download
Backup Local

Note

You only get to see the recordings of events that happened only 150 seconds before or after the selected time indication on the timeline.

9.1.4 Playing the Selected Video Footage

When you have selected a video image, either on the timeline or on event, you can click the play button to watch the footage.

While playing the footage, you can fast forward or rewind, using the control buttons underneath the video playback. Click to return to normal playback.

> ***Note***
>
> The video player plays what is shown on the timeline. If you display only, for example, motion recordings, the player skips the 'empty' time slots in between motion recordings.

To halt the playback, click the stop button. The image will freeze at the time reached in the playback.

To show/hide analytics bounding boxes, click .

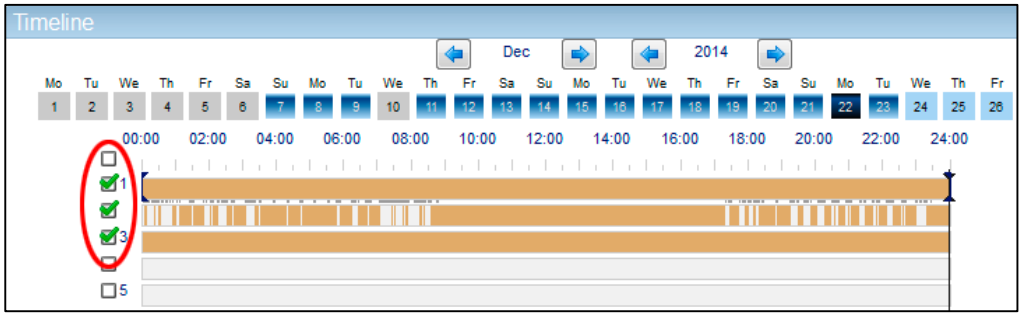
Audio is available if you have enabled audio for the camera (see *Audio IN* on page 35). Drag the slider to adjust the volume level, or click to mute/unmute the sound.

Double-click the video player to get a full screen image. Double-click again to quit the full screen player.

To de-warp images from a 360° panoramic camera, click . For more information, see *360° Camera Images* on page 94.

9.1.5 Synchronised Playback

To watch video footage of multiple cameras (with images of identical time settings), tick the camera timelines you would like to include in the synchronised playback. Choose your time frame and click .



You will automatically get a full screen image with different camera footage.

When you double-click one of the images, this image will be shown in full screen. Double-click it again to return to multiple playback.

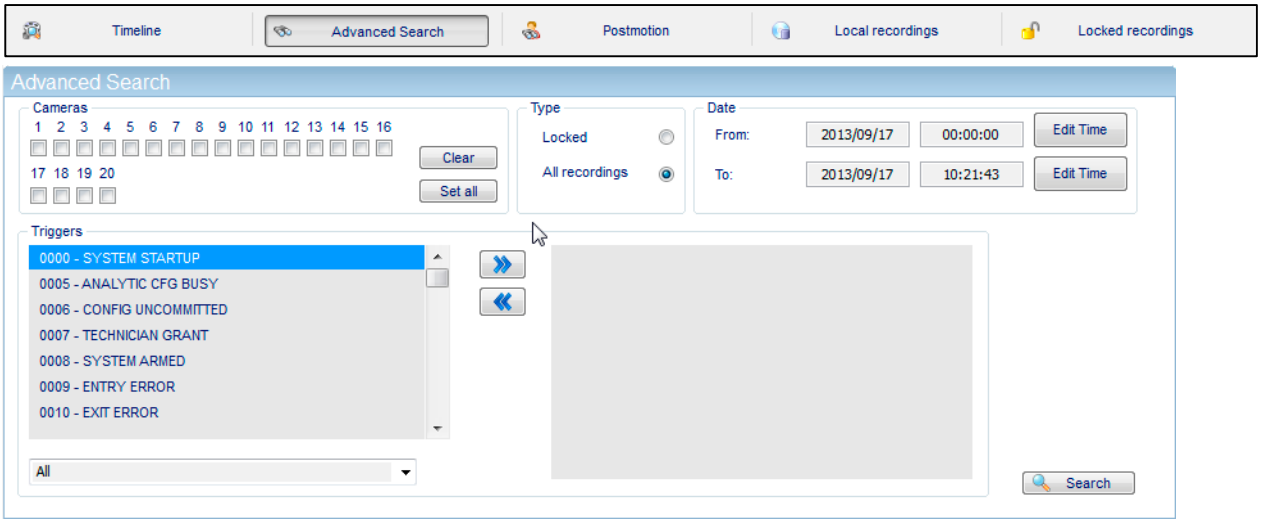
To stop synchronised playback and return to the timeline screen, click the close button in the top right corner, or click the stop button .

You can also click the ‘Info’ button to see the detailed information of each camera under the camera image.

Recorded video
Camera 1 2CIF V:0.00 kB/s A:0.00 kB/s
Camera 2 4CIF V:0.00 kB/s A:0.00 kB/s
Camera 4 CIF V:0.00 kB/s A:0.00 kB/s
Camera 7 CIF V:0.00 kB/s A:0.00 kB/s
Axis Q1755 480x270 V:0.00 kB/s A:0.00 kB/s
V:0.00 kB/s A:0.00 kB/s
2011-05-26 09:38:02
Info

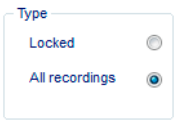
9.2 Searching Recordings via Advanced Search

Click Advanced Search.

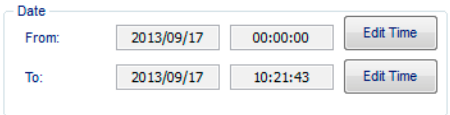


Tick the desired camera. You can tick multiple cameras.

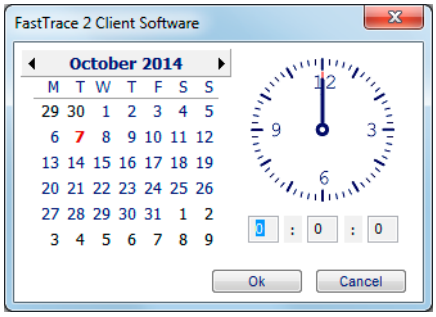
In the *Type* section select whether you want to search all recordings or only locked recordings.



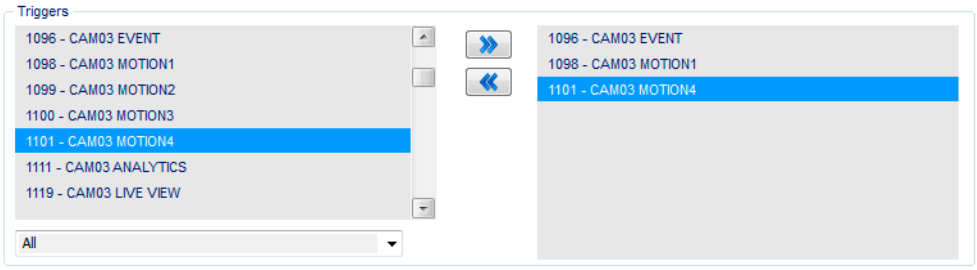
Select the desired time frame for the recordings.



You can manually type the time indication or use the **Edit Time** button to open this window:



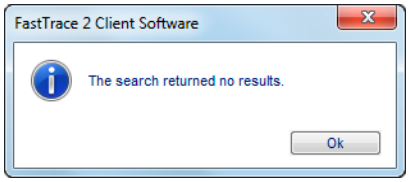
Select the event in the **Triggers** pane and click the blue double arrows button to move the selected event to the pane on the right.



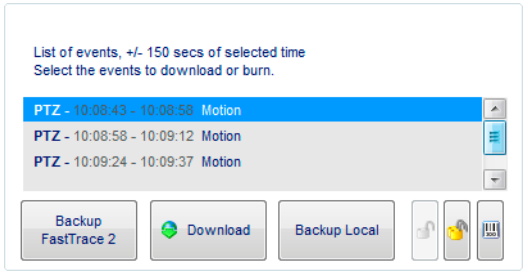
At the bottom left you can filter on the kind of trigger you are looking for. A maximum of 4 triggers can be moved to the search section.

Click **Search** to start searching for recordings.

When you get this popup message, you need to adjust your settings (if you are sure that there should be results).



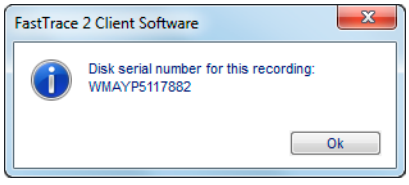
If there are any results matching your search, they will be shown at the top right.


List of events, +/- 150 secs of selected time
Select the events to download or burn.
PTZ - 10:08:43 - 10:08:58 Motion
PTZ - 10:08:58 - 10:09:12 Motion
PTZ - 10:09:24 - 10:09:37 Motion
Backup FastTrace 2
Download
Backup Local

Select the desired recording. You can now watch and/or download this footage.

(For more information, see *Downloading and Storing Selected Video Recordings* on page 89).

If you have multiple hard disks in your video system, you can check on which hard disk the footage has been stored. Select the desired recording and click the button. A popup window appears with the serial number of the hard disk.



Click **OK** to close the message box.

9.3 Searching Recordings via Postmotion

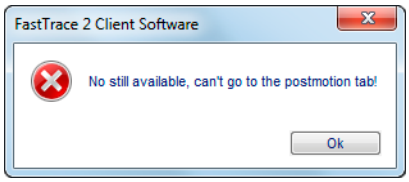
The video recorder does not only store the video footage on the hard disk, it also creates a metadata file describing the contents of the footage. This information allows you to quickly find all sequences in which an object was moving inside a specific area of the camera lens.

Select a desired camera image on the *Timeline* tab.

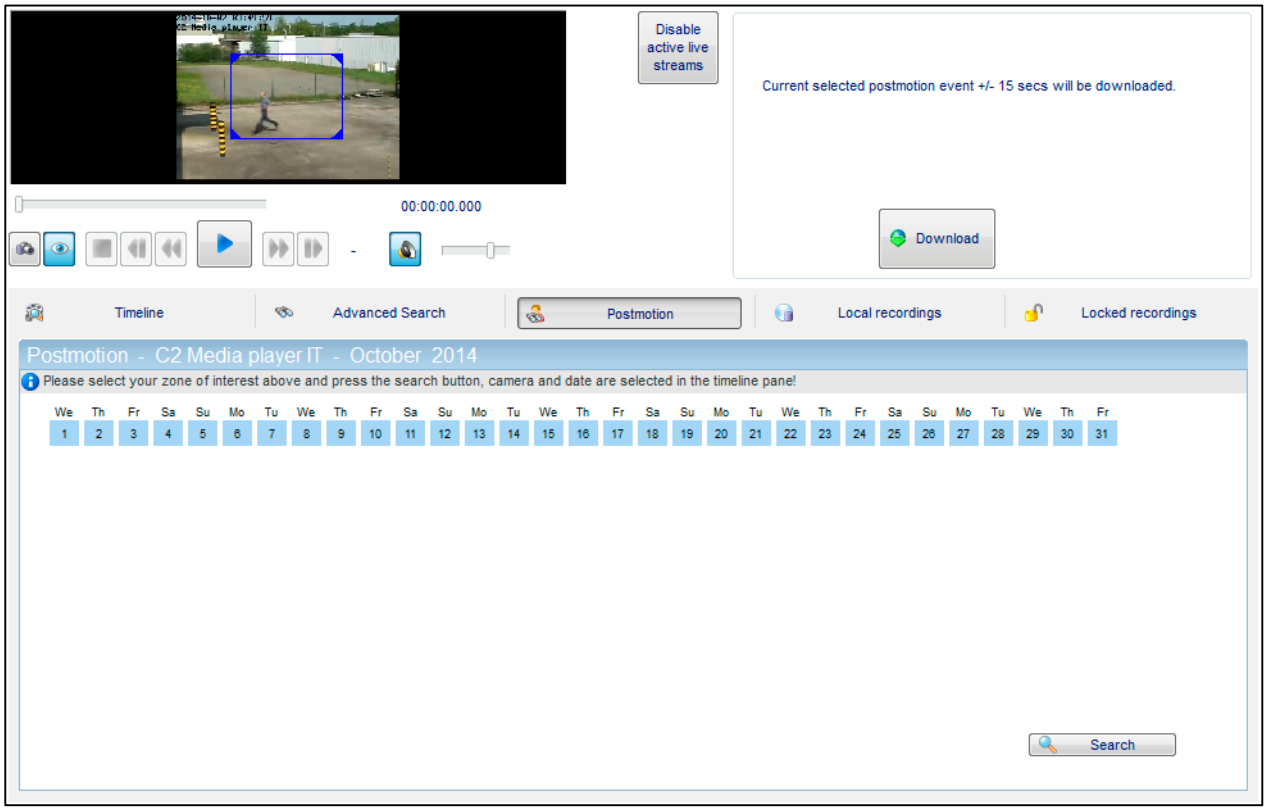
(For more information, see *Searching Recordings on the Timeline* on page 82).

Next, click **Postmotion**.

Normally a still image is automatically available. If no still image has been defined on the timeline tab (e.g. because you did not leave the time to load the memory), you will get this error message:



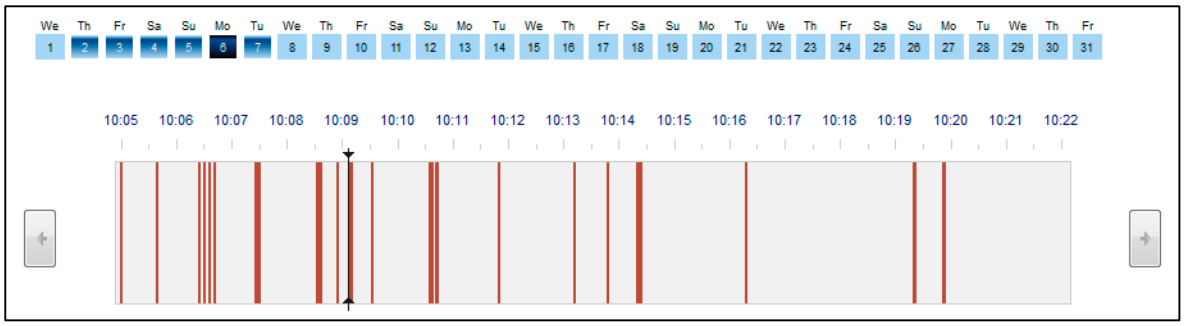
If you did choose an image still (visible in the small screen at the top left), you will get this window:


Disable active live streams
Current selected postmotion event +/- 15 secs will be downloaded.
00:00:00.000
Download
Timeline
Advanced Search
Postmotion
Local recordings
Locked recordings
Postmotion - C2 Media player IT - October 2014
Please select your zone of interest above and press the search button, camera and date are selected in the timeline pane!
Search

In the still image at the top left a blue square appears. This blue square indicates your zone of interest. This will be the zone that is being analysed. Adjust the size and position of the zone if desired and click **Search**.

When the search has been completed, you will get a time scale with the results.

Select the day of interest (only dates that light up dark blue contain recordings). Drag the mouse pointer on the time indication line to zoom in on a specific period.



Click the right mouse button on the time indication line to zoom out to the original result display.

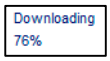
Click a specific recording and the **Play** button to watch that recording. Use the arrow buttons to go to the previous or next recording.

Click **Download** if you want to store the footage in your work folder.

9.4 Downloading and Storing Selected Video Recordings

Select the desired video footage and click **Download**.

You can see the downloading status:

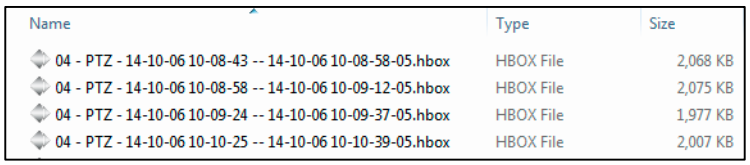


Note

During download, the **Download** button changes:

. Click the button to stop downloading.

The downloaded video footage is stored on your local hard disk in the work folder. The file name contains the camera number, camera name, and the time frame of the recording. The file is stored with the extension ".hbox".



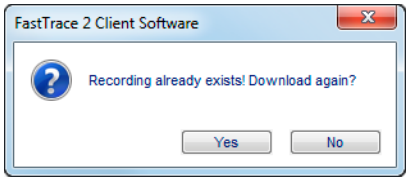
For slow network connections it is recommended to – especially with synchronized playback – disable all live streams in order to increase the download speed. You can disable all active live streams by clicking the **Disable active live streams** button.

To enable live streams again, click **Live Video** in the top menu, and then add the desired cameras to the live view.

Note

When downloading a recording via **Postmotion**, only part of the recording will be stored: the selected time plus about 10 extra seconds.

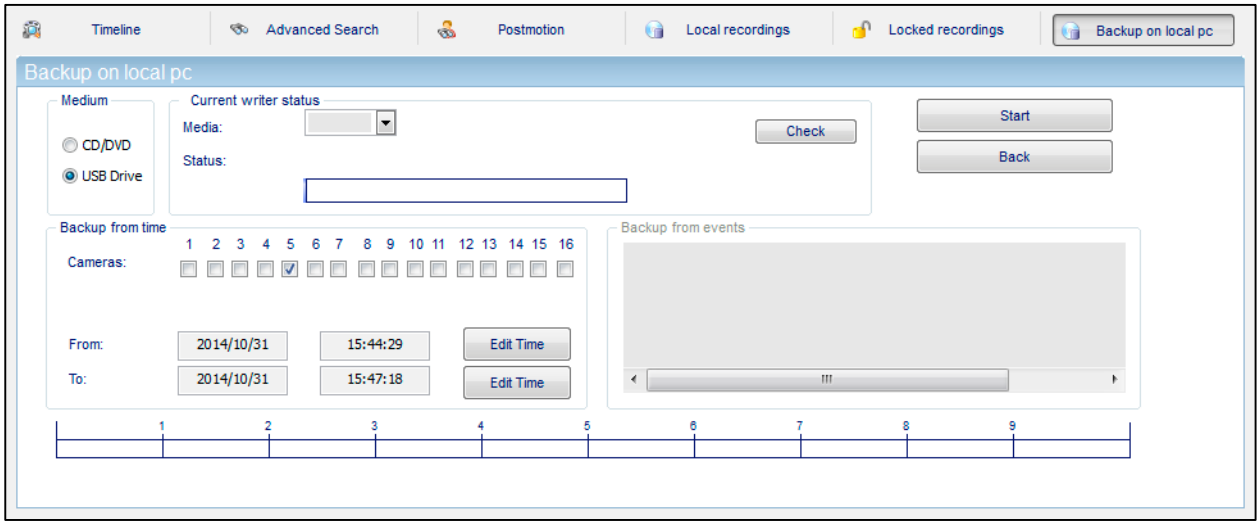
If you have already downloaded the video footage and click the **Download** button again, you will be asked whether you want to download the recording once more:



You can also store video footage as image files on a USB drive of CD/DVD connected to the server or to your local PC.

- Click **Backup to server** to store the video on a USB or CD/DVD drive on the server.
- Click **Backup Local** to store the video on a USB or CD/DVD drive connected to your local PC.

The following screen appears:

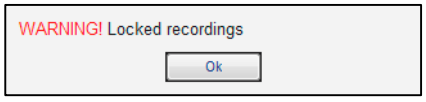


Select the desired storage medium (CD/DVD or USB drive) and tick the desired cameras. Also define the time frame of the recordings you want to store. If storing event recordings, you can select which events you would like to store.

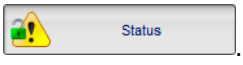
Click **Start** to start burning the video footage to the selected drive. Click **Back** to return to the previous window.

9.5 Locked Recordings

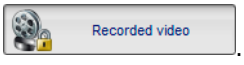
For recordings on event, you can specify to lock the recordings (see *Recording on Event* on page 68). As soon as there is a locked recording, the XOa client displays the following warning message:



Click **OK** to close the message box.

The **Status** button indicates the fault status: 

.

The **Recorded Video** button indicates the presence of locked recordings: 

.

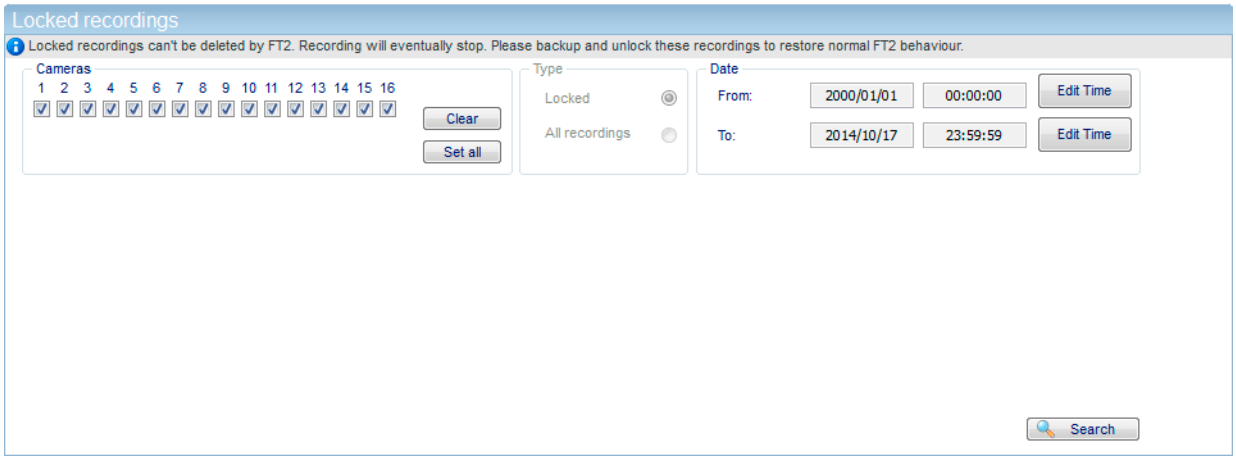
Furthermore, locked recordings trigger the system message 0049 – [SYST] – LOCKED RECORDER (by default linked to the alarm profile NORMAL EVENT).

> ***Caution!***
>
> The RMG cannot delete locked recordings. When it encounters a locked recording during automatic clean-up (for example after 30 days), it stops cleaning up and **also stops recording**.

To prevent that the server stops recording, you must download the locked recordings as soon as you receive the warning message, and then unlock them so that the system can delete them.

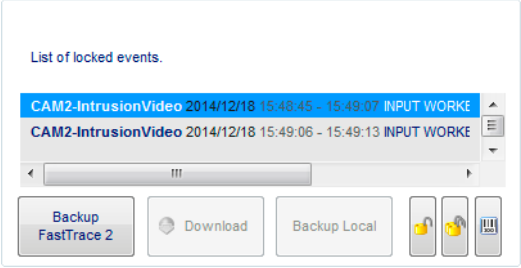
To handle locked recordings, proceed as follows:

1. In the top menu, click **Recorded Video**.
2. Click the **Locked Recordings** tab.



By default, all cameras are selected, and the timeframe is set to cover the full operational time of the server (from the year 2000 until the end of the current day). This makes sure that the system finds all existing locked recordings.

3. Click **Search**. The locked recordings appear in the **List of locked events** box (top right of the screen).


List of locked events.
CAM2-IntrusionVideo 2014/12/18 15:48:45 - 15:49:07 INPUT WORKE
CAM2-IntrusionVideo 2014/12/18 15:49:06 - 15:49:13 INPUT WORKE
Backup FastTrace 2
Download
Backup Local

4. Select the recordings in the list and click **Download**. The system copies the selected recordings to the work folder on your PC. After successful downloading, you can unlock the recordings.
5. To unlock all recordings in the list, click or .
6. Click **Yes** to confirm.

The system can now delete the unlocked recordings and continue with automatic clean-up.

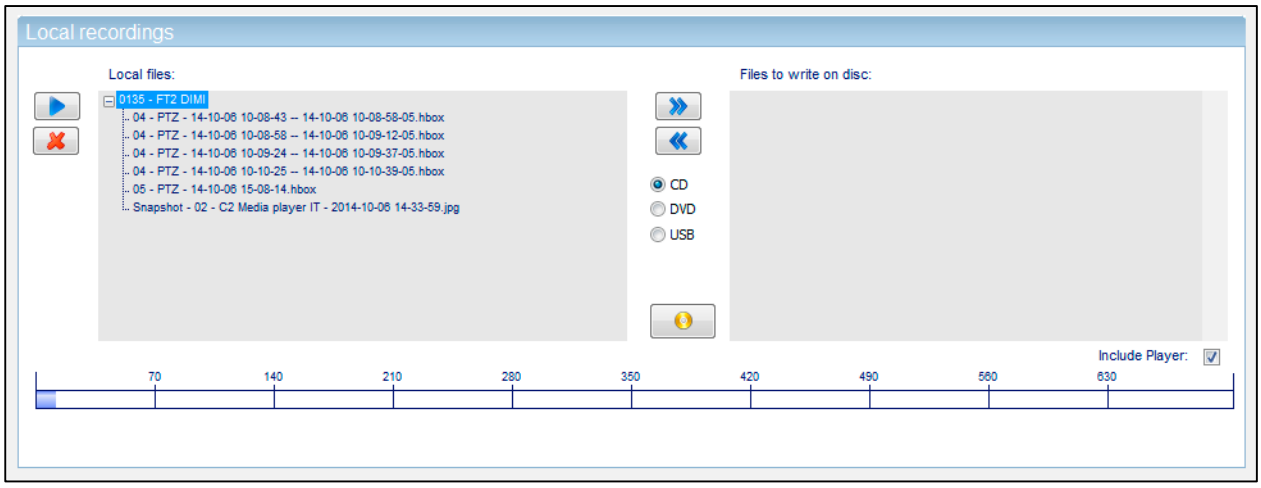
9.6 Managing Local Recordings

All downloaded video recordings are stored in the work folder of the XOa client on your local hard disk (or network folder). Recordings are arranged in subfolders, providing a separate subfolder for each video system. You can recognise the servers by their identification number (1–9999).

This identification number is defined via **System > Behaviour > CMS Alarm transmission**, under **General**, in the **Server Unit ID** box.

To watch locally stored video recordings, click **Local recordings**.

The following screen appears:



Unfold the desired video system folder and select a recording. You now have several options:

	Playback the selected recording.
	Delete the selected recording.
	Add the selected recording to the “burning” list. This is the list of files that you want to store (burn) on CD, DVD, or USB.
	Delete the selected recording from the “burning” list. This is the list of files that you want to store (burn) on CD, DVD, or USB.
	Select the desired drive on which you want to burn the video recordings.
	Start burning the video recordings from the burning list to the selected drive.

If you select the **Include Player** check box (at the bottom right), you will also burn all software required to watch the video recordings, to the CD/DVD/USB. That way you can play the recordings on any Windows compatible computer.

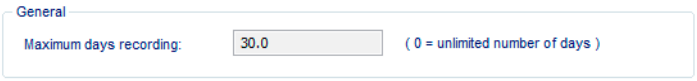
Note

If you want to play the video recording in full screen, double-click the image (with the left mouse button). Double-click the full screen image to return to normal view.

9.7 Automatically Erasing Old(er) Video Recordings

Local legal requirements (variable and depending on state and region) may necessitate the video system to delete all recordings after some predefined period. The video recordings may only be stored on the hard disk for a limited period of time. When that period of time has passed, the recordings should be erased from the hard disk.

You can activate this function via **System > Behaviour > Recordings Behaviour**.



Click **Save** to apply the new settings.

Caution!

FastTrace cannot automatically erase recordings on event that are locked. You must unlock these recordings manually, so that FastTrace can erase them. If not, FastTrace stops erasing **and recording** when it encounters the first locked recording during clean-up.

For more information, see *Locked Recordings* on page 90.

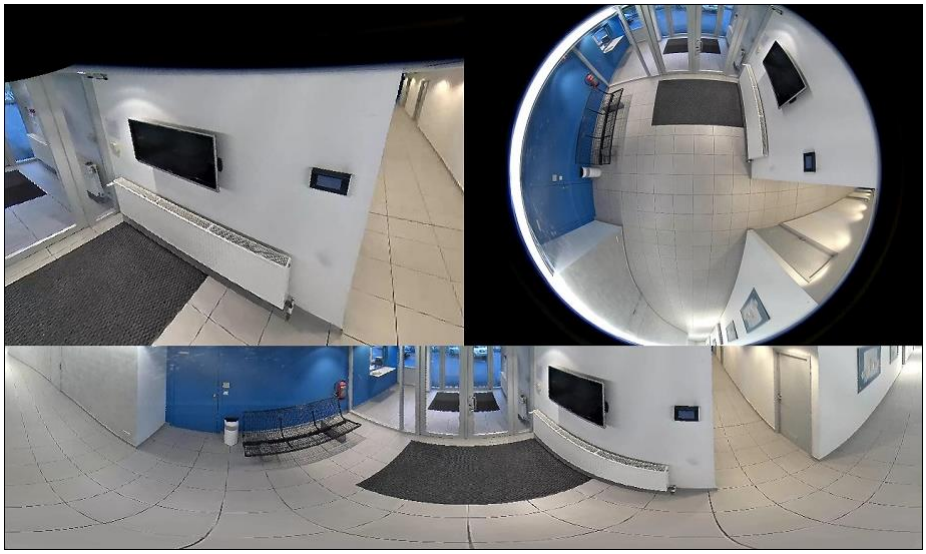
10 360° Camera Images

You can de-warp 360° camera images:

- From the live view
- From recorded video view.

To de-warp 360° camera images, proceed as follows:

1. If you start from the **Live Video** screen, right-click the camera image and click **Dewarp mode**.
2. If you start from recorded video viewing, click **360**. The following screen appears:



The screen displays:

- The original 360° image at the top right
- The de-warped image at the bottom
- Detail view of the de-warped image in the top left.

3. Proceed as follows:
   - Click anywhere in the 360° image or in the de-warped image to see the detail in the top left corner.
   - Press and hold the mouse button to zoom in. Press and hold Shift, and press and hold the mouse button to zoom out.
4. To return to the normal view:
   - In the **Live Video** screen, right-click the camera image again and click **Dewarp mode**.
   - In the recorded video screen, click **360**.

11 Arm/Disarm Schedule

Events on the RMG can be classified in the following groups:

- System messages: these are internal events (e.g. hard disk error, power supply fault, communication error…)
- Camera messages (e.g. video signal missing, contrast level too low, motion detected…)
- Network inputs: alarm inputs connected to external Net I/O modules
- Inputs: alarm inputs connected to the OTB I/O card, accessible at the back of the video system;
- Virtual inputs: events detected on interconnected S3100 security panels.
- Workbits: calculated bits that provide alarm information. A combination of inputs can trigger a workbit.

Events have to be handled in a different way when the building is left unattended. Therefore, the building has to be armed. Arming can be done in three ways:

1. Automatically according to a schedule. See the setup procedure further below.
2. Manually, when a user activates a switch.
3. The CMS can execute the DN command line in Telnet (hint: type HE for syntax help in Telnet).

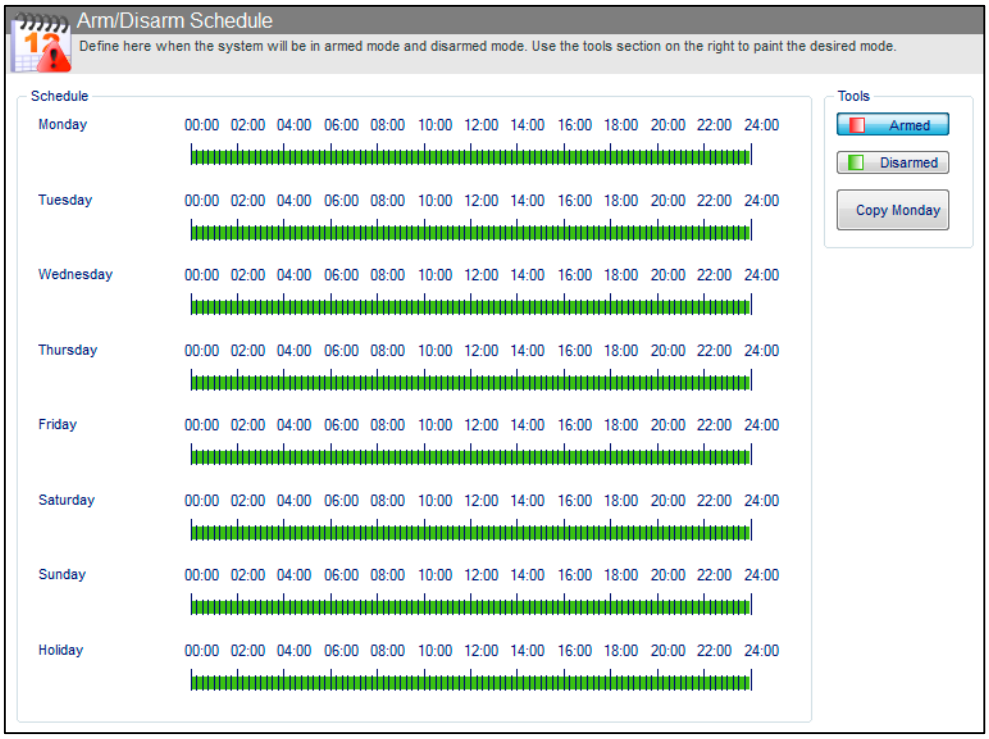
To define the behaviour of an alarm input during armed and disarmed state, modify the alarm profile that is assigned to this input.

Note

It is possible for other software developers to use the SDK (software development kit) in order to arm/disarm a building.

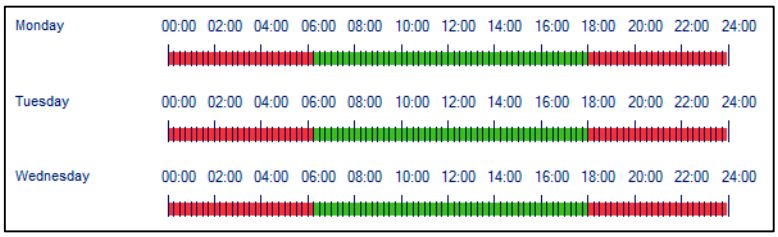
To set up the schedule for automatically arming/disarming a building, proceed as follows:

1. Choose **System > Behaviour > Arm/Disarm schedule**.



By default the system is always disarmed, indicated by the green bars. You can set up a different schedule for each day of the week, and for holidays. Tip: you can set up the schedule once for Mondays, and then copy it to the other days.

2. Indicate the desired armed/disarmed states on the time bar as follows:
   - To specify when the system is armed, click **Armed**, and then drag the mouse over the time bar. The selected period appears in red.
   - To specify when the system is disarmed, click **Disarmed**, and then drag the mouse over the time bar. The selected period appear in green.

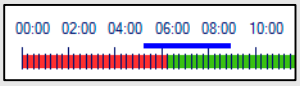


3. To copy the schedule from Monday to all other days, click **Copy Monday**.
4. Click **Save**.

The video system shall now automatically arm/disarm according to your schedule. A switch can always force the system to another state.

Note

To zoom in on a part of the day, position the mouse pointer on the time scale, press the left mouse button and drag the mouse to the right (drawing a blue line). Release the mouse button.



To zoom out, right-click the time bar.

12 Alarm Profiles

12.1 About Alarm Profiles

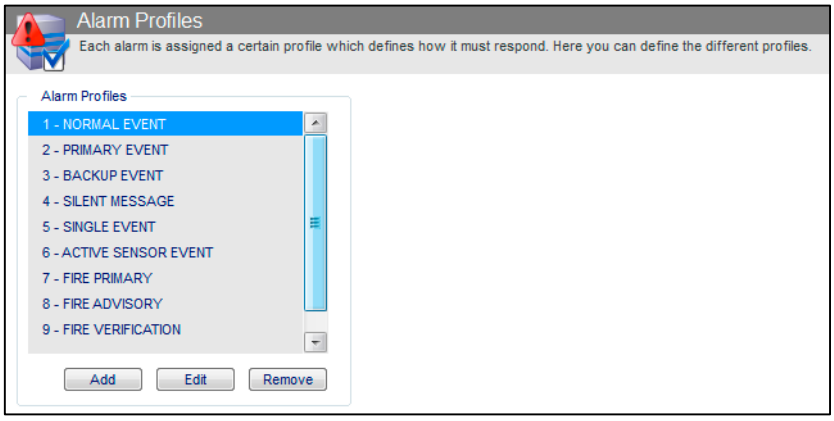
An alarm profile defines how the server responds when an alarm or event is triggered. It defines the transmission channel(s), if the alarm is transmitted when the system is armed/disarmed, whether or not the alarm is repeated, etc. The server comes with 10 standard alarm profiles. It is not recommended to change the default profiles. It is better to create new profiles instead.

12.2 Adding a New Profile

You can create up to 32 different alarm profiles.

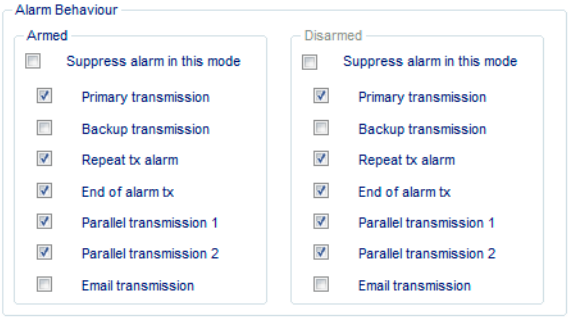
To add a new alarm profile, proceed as follows:

1. Choose **System > Behaviour > Alarm Profiles**.


Alarm Profiles
Each alarm is assigned a certain profile which defines how it must respond. Here you can define the different profiles.
Alarm Profiles
1 - NORMAL EVENT
2 - PRIMARY EVENT
3 - BACKUP EVENT
4 - SILENT MESSAGE
5 - SINGLE EVENT
6 - ACTIVE SENSOR EVENT
7 - FIRE PRIMARY
8 - FIRE ADVISORY
9 - FIRE VERIFICATION
Add
Edit
Remove

2. Click **Add**.
3. Provide the following settings:

Parameter	Description
Profile name	Enter a description (max 20 characters) for the alarm profile. It is recommended to use a meaningful and relevant description.
Active sensor (I201)	If ticked, input I201 – if active – will be triggered. Input I201 can be used to inform the user that some sensors are still active. This prevents arming the system while sensors are still in alarm. (see note underneath)
Profile type	Assign a profile type to the new alarm profile: • 0 – Alarm: this is a generic type; you can change any setting. Use it to customise the alarm profile to your every need. • 1 – Fire primary: you can change all settings for this profile type, except the operational state (fixed to **Armed/disarmed**) and the repeat alarm (**Repeat tx alarm** fixed selected). Use this profile type if you need a custom alarm profile for primary fire alarms. • 2 – Fire advisory: you can change all settings for this profile type, except the operational state (fixed to **Armed/disarmed**) and the repeat alarm (**Repeat tx alarm** fixed selected). Use this profile type if you need a custom alarm profile for advisory fire alarms. • 3 – Fire verification: you can change all settings for this profile type, except the operational state (fixed to **Armed/disarmed**) and the repeat alarm (**Repeat tx alarm** fixed selected). Use this profile type if you need a custom alarm profile for fire verification alarms. • 4 – Fire trouble: you can change all settings for this profile type, except the operational state (fixed to **Armed/disarmed**) and the repeat alarm (**Repeat tx alarm** fixed selected). Use this profile type if you need a custom alarm profile for fire trouble alarms.

Parameter	Description
Operational state	• Disarmed: inputs are only monitored when the system is disarmed; consequently alarms will only be transmitted when the system is disarmed. • Armed: inputs are only monitored when the system is armed; consequently alarms will only be transmitted when the system is armed. • Armed/disarmed: inputs are always monitored; consequently alarms will always be transmitted.
Alarm Behaviour	• Suppress alarm in this mode: it is possible to suppress alarms in one or both operational states. When you activate this option, the alarms that have been assigned to this profile will no longer be activated during the suppression. By doing this you will disable event-based recordings, emailing, PTZ triggers, logging…. ***Caution!*** Suppressing alarms is **not recommended**. Do not use this option unless specifically asked to do so, for example by Xtralis Support staff. • Primary transmission: send events to the CMS via the main connection; • Backup transmission: send events to the CMS via the provided backup connection. The backup connection will only be used if transmission on the main connection has failed! • Repeat tx alarm: send reminders at regular times (each 15 minutes*) if the alarm is sustained. • End of alarm tx: send message to CMS when input returns to normal state (negative alarm). • Parallel transmission 1: sends event/message via parallel transmission 1. • Parallel transmission 2: sends event/message via parallel transmission 2. • Email transmission: sends event/message via email. 

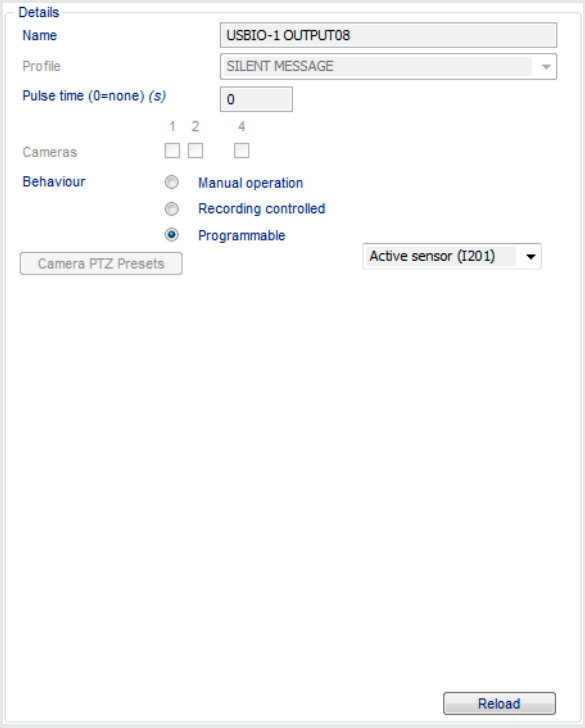
* The following alarm messages will only be repeated once every 24 hours:

- 65 license expired
- 66 license out of sync
- 67 application stopped
- 511 general isolation

1. Click **Save** to apply the new settings.

Note

To activate an output on input I201, open **System > Behaviour > Input/Output behaviour**, select an output (filter on **Outputs: on the box** to see only the physical outputs) and choose Programmable. Select **Active sensor (I201)** in the list.



All sensors assigned to an alarm profile that triggers I201, have to return to idle state in order to reset the selected output. When this condition is fulfilled, the user can arm the video system without triggering a false alarm.

12.3 Deleting an Alarm Profile

Note

You cannot delete the default alarm profiles, or alarm profiles that are in use (= assigned to events).

To delete an alarm profile, proceed as follows:

1. Click the alarm profile in the list, and then click **Remove**.
2. Click **Yes** to confirm.
3. Click **Save**.

12.4 Default Profiles

The server comes with 10 standard alarm profiles:

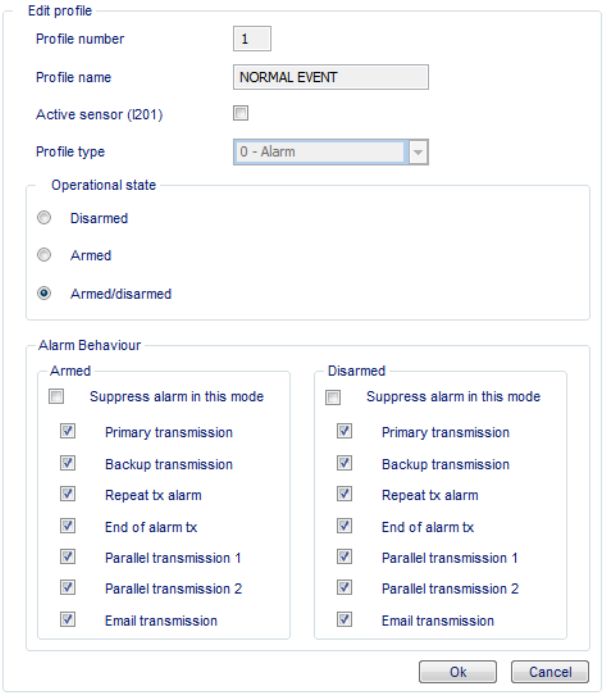
- 1 – NORMAL EVENT
- 2 – PRIMARY EVENT
- 3 – BACKUP EVENT
- 4 – SILENT MESSAGE
- 5 – SINGLE EVENT
- 6 – ACTIVE SENSOR EVENT
- 7 – FIRE PRIMARY
- 8 – FIRE ADVISORY
- 9 – FIRE VERIFICATION
- 10 – FIRE TROUBLE

Alarm profiles 7–10 are only available if you have installed a SmokeTrace license on your server.

To modify the behaviour of alarm transmission of inputs, you need to modify the associated alarm profile of the input. It is however **not recommended to modify the default alarm profiles**. It is better to create a new alarm profile with different settings. See *Adding a New Profile* on page 97.

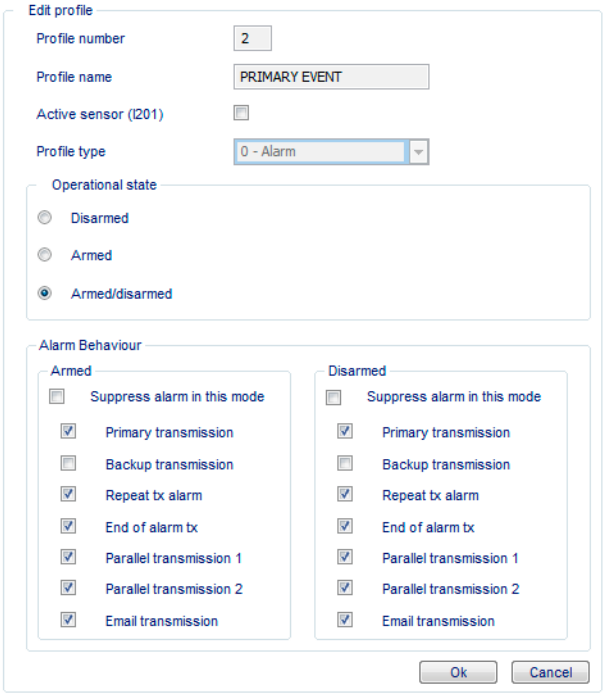
12.4.1 Normal Event Profile

A normal event profile is defined to send alarms for all detections to **all transmission destinations**: primary, backup, parallel, and email. It does not take the operational state into account: the alarm will be generated in both armed and disarmed state. Furthermore, the alarm transmission will be repeated every 15 minutes as long as the alarm is sustained. When the end of alarm is detected, a new alarm message will be sent to indicate that the alarm is no longer sustained.
The profile type is **0 – Alarm** (generic profile type). Note that you cannot modify the profile type of the standard alarm profiles.



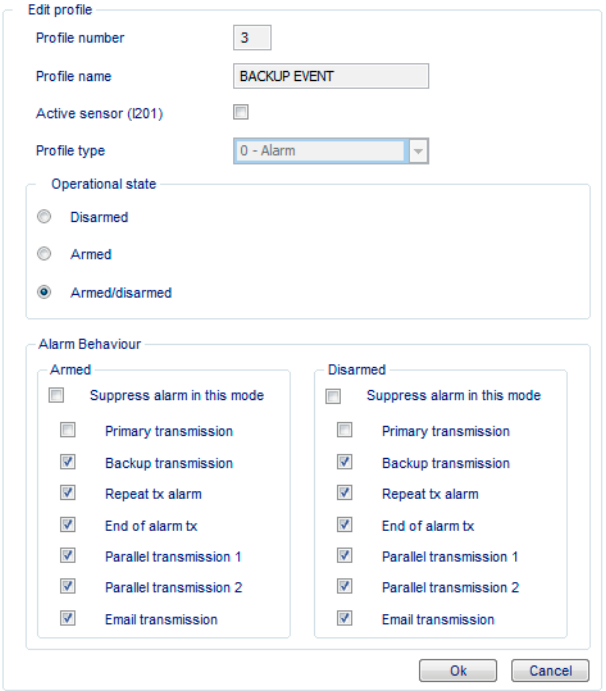
12.4.2 Primary Event Profile

A primary event profile is defined to send alarms for all detections to the **primary** transmission destination, but **not the backup** transmission. It also sends to the parallel and email transmission destinations. It does not take the operational state into account: the alarm will be generated in both armed and disarmed state. Furthermore, the alarm transmission will be repeated every 15 minutes as long as the alarm is sustained. When the end of alarm is detected, a new alarm message will be sent to indicate that the alarm is no longer sustained.
The profile type is **0 – Alarm** (generic profile type). Note that you cannot modify the profile type of the standard alarm profiles.



12.4.3 Backup Event Profile

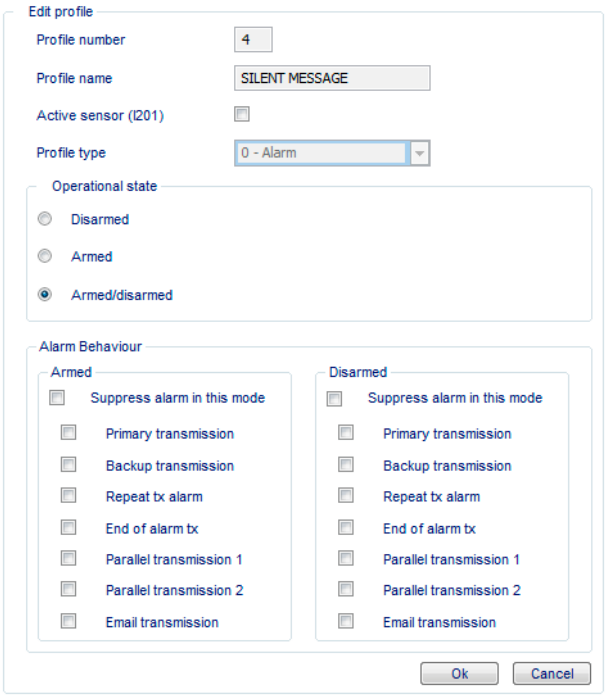
A backup event profile is defined to send alarms for all detections to the **backup** transmission destination, but **not the primary** transmission. It also sends to the parallel and email transmission destinations. It does not take the operational state into account: the alarm will be generated in both armed and disarmed state. Furthermore, the alarm transmission will be repeated every 15 minutes as long as the alarm is sustained. When the end of alarm is detected, a new alarm message will be sent to indicate that the alarm is no longer sustained.
The profile type is **0 – Alarm** (generic profile type). Note that you cannot modify the profile type of the standard alarm profiles.



12.4.4 Silent Message Profile

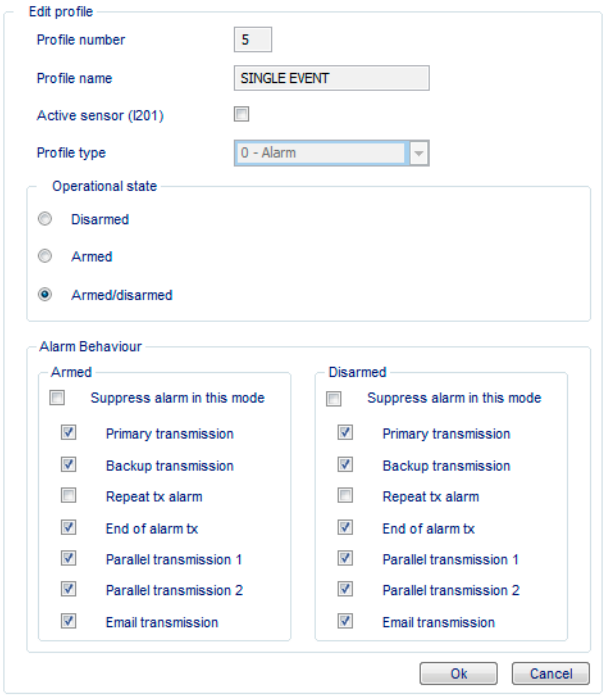
A silent message profile is defined to generate an alarm, but the alarm is **not sent to any transmission destination**.

The alarm message is generated in both armed and disarmed state, but will not be sent to an alarm management system (like M3000). The idea behind this type of alarm is to get an overview in the log file. The profile type is **0 – Alarm** (generic profile type). Note that you cannot modify the profile type of the standard alarm profiles.



12.4.5 Single Event Profile

A single event profile is defined to send alarms for all detections to **all transmission destinations**. It does not take the operational state into account: the alarm will be generated in both armed and disarmed state. When the end of alarm is detected, a new alarm message will be sent to indicate that the alarm is no longer sustained. The alarm will, however, **not be repeated** every 15 minutes as long as the alarm is sustained. The profile type is **0 – Alarm** (generic profile type). Note that you cannot modify the profile type of the standard alarm profiles.

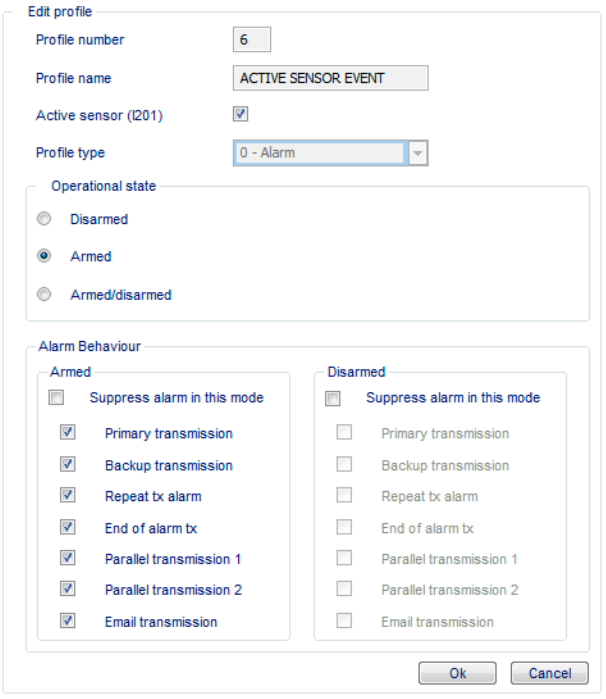


12.4.6 Active Sensor Event Profile

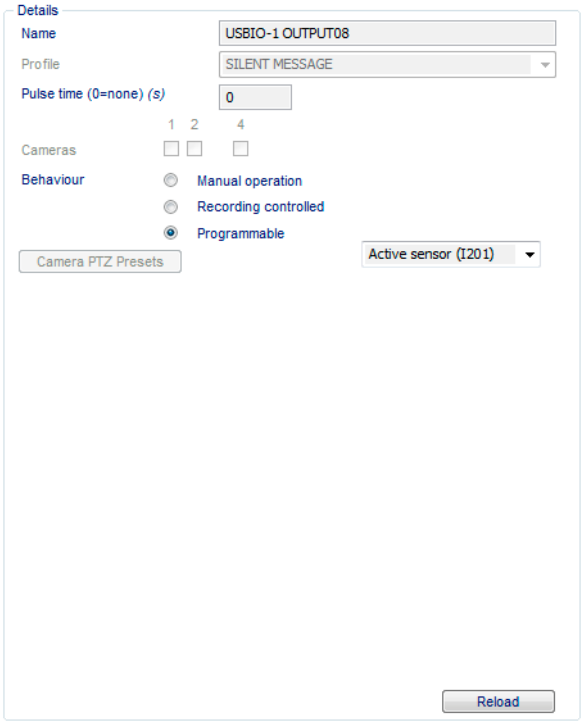
An active sensor event profile is defined to send alarms for all detections to **all transmission destinations**. This alarm is only generated when the operational state of the video system is **armed**.

This alarm profile also **triggers input I201**, thus activating the active sensor. Input I201 is used to inform the user that some sensors are still active. This will prevent arming the system while sensors are still in alarm.

Furthermore, the alarm transmission will be repeated every 15 minutes as long as the alarm is sustained. When the end of alarm is detected, a new alarm message will be sent to indicate that the alarm is no longer sustained.
The profile type is **0 – Alarm** (generic profile type). Note that you cannot modify the profile type of the standard alarm profiles.



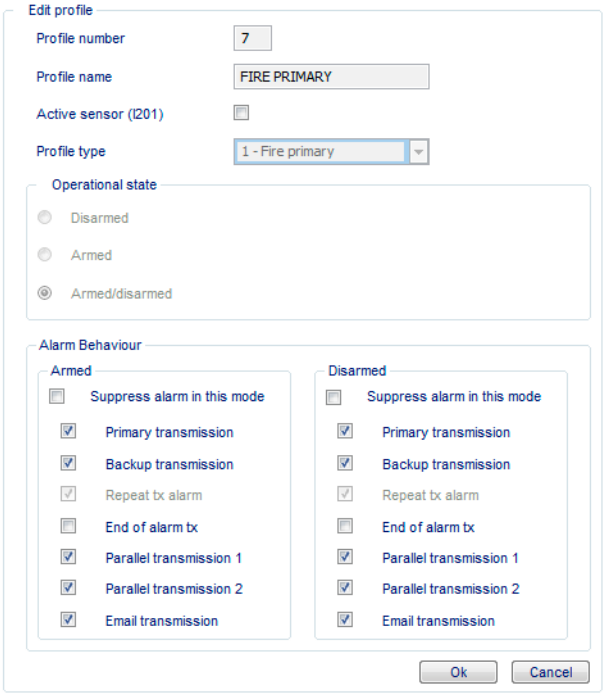
To activate an output on input I201, open **System > Behaviour > Input/Output behaviour**, select an output (filter on *On the box* outputs to see only the physical outputs) and choose Programmable. Select **Active sensor (I201)** in the list.



All sensors assigned to an alarm profile that triggers I201, have to return to idle state in order to reset the selected output. When this condition is fulfilled, the user can arm the video system without triggering a false alarm.

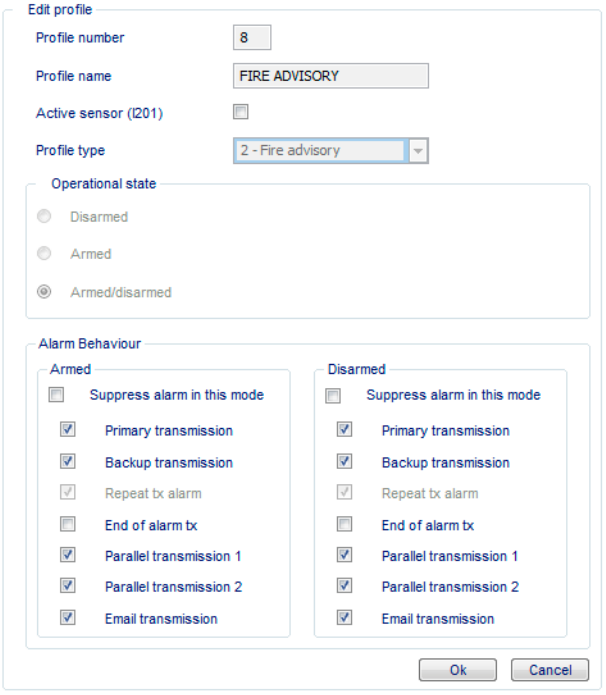
12.4.7 Fire Primary Profile

The fire primary profile is used with fire detection systems. You use it to send alarm messages to all transmission destinations when a primary fire detection device detects fire. The profile sends messages in both armed and disarmed states. It sends the alarm message again every 15 minutes as long as the alarm is active. When the system detects the end of alarm, it **does not send** a new message indicating that the alarm is no longer active. Note that you cannot switch off the repeat alarm.
The profile type is **1 – Fire primary**. Note that you cannot modify the profile type of the standard alarm profiles.



12.4.8 Fire Advisory Profile

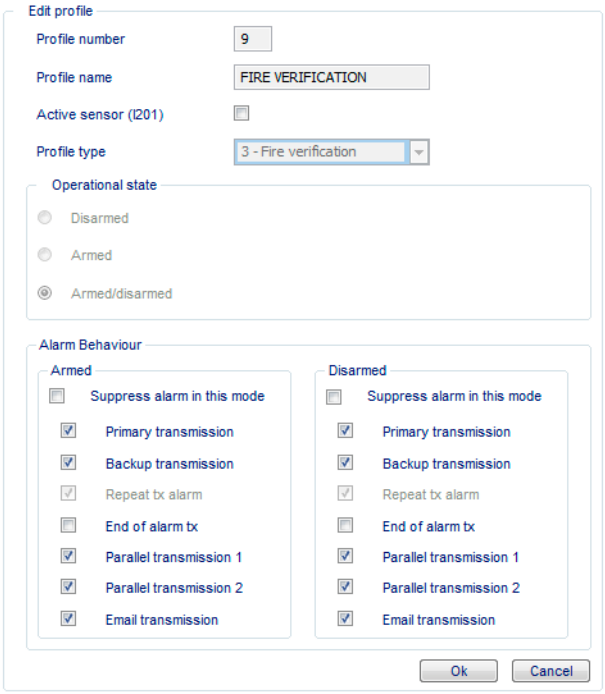
The fire advisory profile is used with fire detection systems. You use it to send alarm messages to all transmission destinations when an advisory fire detection device (such as an OSID Imager) detects fire. The profile sends messages in both armed and disarmed states. It sends the alarm message again every 15 minutes as long as the alarm is active. When the system detects the end of alarm, it **does not send** a new message indicating that the alarm is no longer active. Note that you cannot switch off the repeat alarm. The profile type is **2 – Fire advisory**. Note that you cannot modify the profile type of the standard alarm profiles.



12.4.9 Fire Verification Profile

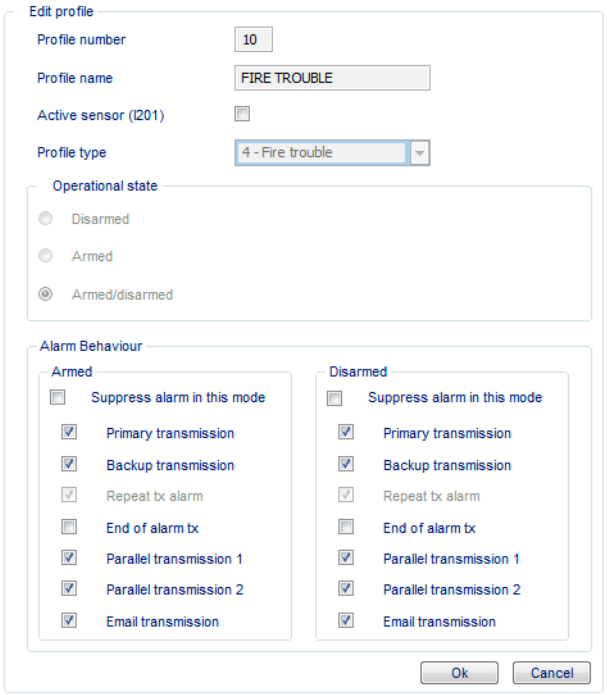
The fire verification profile is used with fire detection systems. You use it to send alarm messages to all transmission destinations when SmokeTrace has verified the presence of smoke. The profile sends messages in both armed and disarmed states. It sends the alarm message again every 15 minutes as long

as the alarm is active. When the system detects the end of alarm, it **does not send** a new message indicating that the alarm is no longer active. Note that you cannot switch off the repeat alarm.
The profile type is **3 – Fire verification**. Note that you cannot modify the profile type of the standard alarm profiles.



12.4.10 Fire Trouble Profile

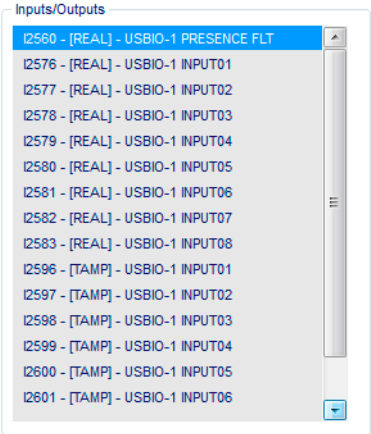
The fire trouble profile is used with fire detection systems. You use it to send fault messages to all transmission destinations when there is a fault in the fire detection system. The profile sends messages in both armed and disarmed states. It sends the message again every 15 minutes as long as the fault is active. When the system detects the end of the fault condition, it **does not send** a new message indicating that the fault is no longer active. Note that you cannot switch off the repeat alarm.
The profile type is **4 – Fire trouble**. Note that you cannot modify the profile type of the standard alarm profiles.



13 Input/Output Behaviour

13.1 Alarm Input Behaviour

To define alarm inputs, open **System > Behaviour > Input/Output Behaviour**. Select an input from the list.

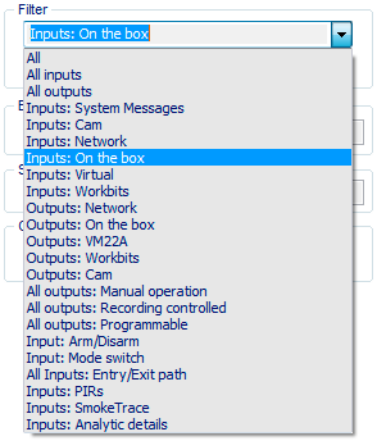

Inputs/Outputs
I2560 - [REAL] - USBIO-1 PRESENCE FLT
I2576 - [REAL] - USBIO-1 INPUT01
I2577 - [REAL] - USBIO-1 INPUT02
I2578 - [REAL] - USBIO-1 INPUT03
I2579 - [REAL] - USBIO-1 INPUT04
I2580 - [REAL] - USBIO-1 INPUT05
I2581 - [REAL] - USBIO-1 INPUT06
I2582 - [REAL] - USBIO-1 INPUT07
I2583 - [REAL] - USBIO-1 INPUT08
I2596 - [TAMP] - USBIO-1 INPUT01
I2597 - [TAMP] - USBIO-1 INPUT02
I2598 - [TAMP] - USBIO-1 INPUT03
I2599 - [TAMP] - USBIO-1 INPUT04
I2600 - [TAMP] - USBIO-1 INPUT05
I2601 - [TAMP] - USBIO-1 INPUT06

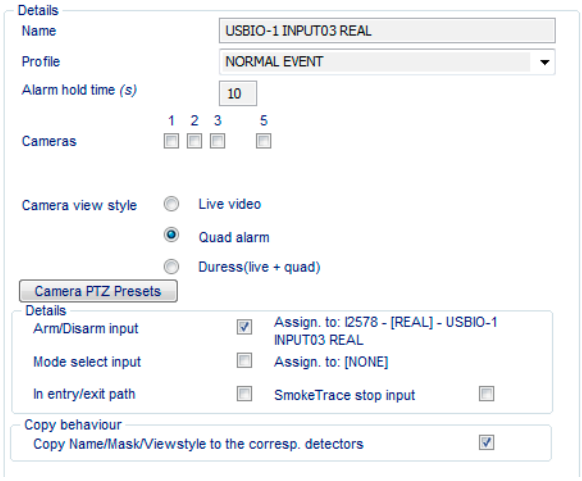
The input has to belong to one of these groups:

- On the box: inputs and outputs on the OTB I/O cards, with alarm and tamper state; 20 inputs on the first set (= Main I/O and Extension I/O card), 20 inputs on the second set (Main I/O and Extension I/O card).
- Network: inputs and outputs on Net I/O modules, connected to the Ethernet (local network).
- System messages: internal events and states, such as hard disk error, modem error…
- Cam: camera alarms, including “no video alarm”, “contrast error”, and “motion alarm”.
- Virtual: events detected on the interconnected S3100 alarm panel. Virtual inputs are selected by alarm profile (e.g. input activated upon motion on camera 1 or alarm on input 2 of the I/O card).
  (For more information, see the *S3100 Technical Manual*.)
- Arm/Disarm: all inputs that have been programmed for arming/disarming
- Mode Switch: all inputs that have been programmed for mode switching.
- Entry/Exit path: all inputs that have been programmed within the entry/exit path (delayed events).
- Workbits: calculated bits that provide alarm information. A combination of inputs can trigger a workbit.

Note

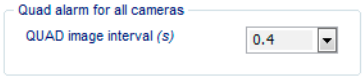
Since the number of inputs and outputs is very long, it might be easier to find the desired input by limiting the list. To limit the list you can use the filter function:





Parameter	Description
Name	Enter a name (max 20 characters) to describe the alarm. It is recommended to use a description that is meaningful and relevant.
Profile	Select an alarm profile. This alarm profile defines the behaviour of the input.
Alarm Hold time	This sets the minimum time of activation of the alarm (in seconds). End-of-alarm will only be detected after this delay. This parameter will suppress a flow of events caused by a rattling alarm contact.
Cameras	Select the desired cameras. Choose cameras that might reveal important information about the event.
Camera view style	Select the video information that should be available to the CMS. • Live video: the CMS can open a connection with the site to watch live images on the relevant cameras; • Quad: the CMS can retrieve pictures from the video system (3 stills are stored on the video system, taken from the relevant camera, with an adjustable interval); • Duress: both live images and pictures are available.

To set the time between successive pictures, choose **System > Behaviour > Input/Output Behaviour** and select the desired interval in the **Quad image interval (s)** box. The value is expressed in seconds.



Caution!

This quad interval setting applies to **all cameras**, and therefore to **all applications**. Different applications may have different ideal quad intervals. For intrusion detection, you may require a short interval, whereas for smoke verification you may want a longer interval. In this case, you have to find a compromise that yields acceptable results for all applications. **Always test** the selected setting.

Arm/Disarm input	Tick this option if the input is used to arm and disarm the system.
Mode select input	Tick this option if the input is used to switch the video system to a defined operation mode (see *Operational Mode with Manual Selection* on page 64). The mode of operation affects the behaviour of video recording!

In entry/exit path (value in seconds)	Tick this option if the alarm has to be delayed. The delay is specified by the parameter '*Entry/Exit hold time delay'*. On entry to the building, the video system has to be disarmed within this time to prevent alarms on the delayed inputs. On exit, the building has to be abandoned within this time counting from the moment when it is armed.

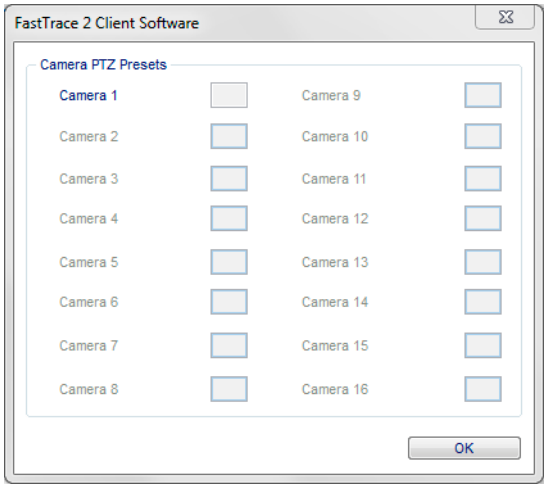
Modify the alarm parameters of the selected input and click **Save** to apply the new settings.

13.2 PTZ via I/O

It is possible to define PTZ preset positions via an input. Open the *Input/Output behaviour* window via **System > Behaviour > Input/Output behaviour**.

Select the desired input and click **Camera PTZ Presets**.

You will get the following popup window:



All PTZ cameras can be provided with 1 specific PTZ preset. When an input is triggered, the camera will move to the configured PTZ preset position. The alarm message will be delayed, however, until the PTZ preset positioning time has expired. This is done to make sure no blurry images are recorded.

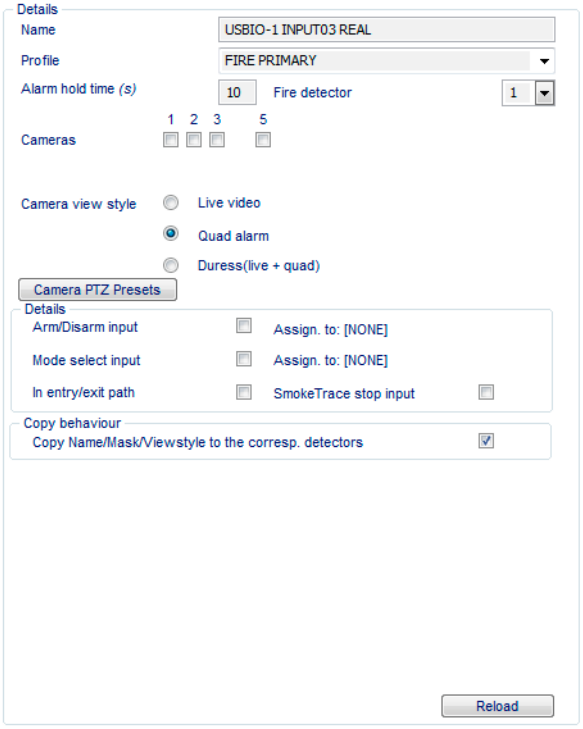
Note

It is not possible to define camera PTZ presets for system inputs, except for SYSTEM ARMED, ENTRY ERROR, EXIT ERROR, GENERAL MODE 1–4, and FIRE SYSTEM FAULT.

13.3 Connecting Fire Detectors

You can connect up to 20 fire detectors to the server. These detectors can either be connected to real inputs on the server or via Net I/O modules.

Open the *Input/Output behaviour* window via **System > Behaviour > Input/Output Behaviour**. Choose a fire event profile and attribute a fire detector number.

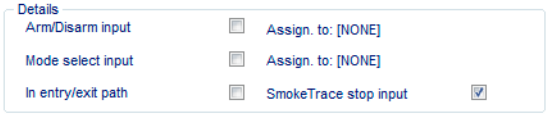


You can tick the option – by default this option is ticked already – *Copy Name/Mask/Viewstyle to the corresp. detectors* to make sure that all modifications are automatically copied to the corresponding detectors.

How many inputs from the same detector you can configure, depends on the type of the fire detector. Please consult the technical documentation of the specific detector for more information.

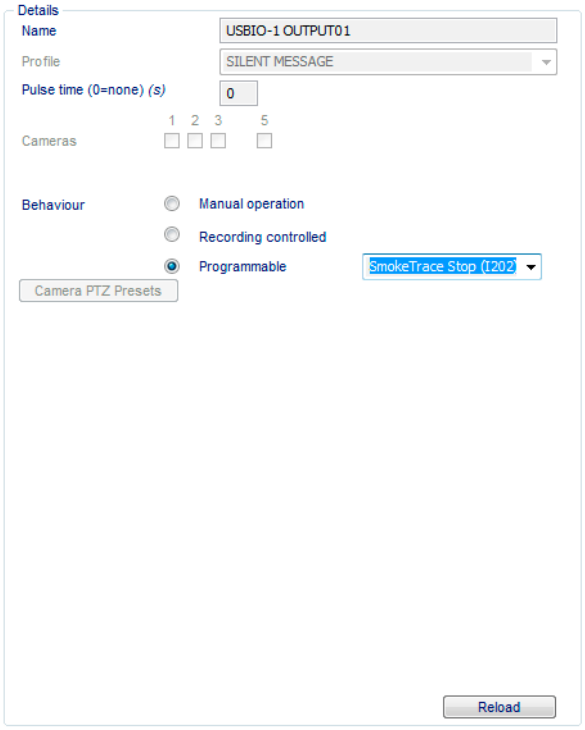
13.3.1 Fire Reset Input and Output (SmokeTrace Stop Input)

You can configure an input as fire reset input. This means that when this input is activated an output will be activated as a consequence. The output will reset all fire detectors.



To define the fire reset output, proceed as follows:

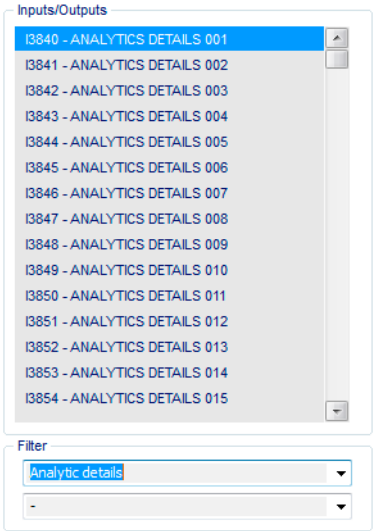
1. Select an output from the list.
2. Set **Behaviour** to **Programmable**.
3. Select **SmokeTrace Stop (I202)** in the list.



To reset the fire detectors you can also use the command ***GR,fire*** (in Telnet or Hyperterminal).

13.4 IntrusionTrace Alarms

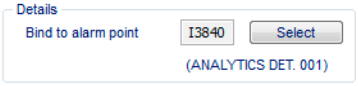
For each camera a set of 16 extra alarms have been created to use with IntrusionTrace. These alarms provide extra information concerning the IntrusionTrace detection on a camera. The alarms can also be used for example to trigger PTZ cameras to zoom in on the detected area on an IntrusionTrace camera.


Inputs/Outputs
I3840 - ANALYTICS DETAILS 001
I3841 - ANALYTICS DETAILS 002
I3842 - ANALYTICS DETAILS 003
I3843 - ANALYTICS DETAILS 004
I3844 - ANALYTICS DETAILS 005
I3845 - ANALYTICS DETAILS 006
I3846 - ANALYTICS DETAILS 007
I3847 - ANALYTICS DETAILS 008
I3848 - ANALYTICS DETAILS 009
I3849 - ANALYTICS DETAILS 010
I3850 - ANALYTICS DETAILS 011
I3851 - ANALYTICS DETAILS 012
I3852 - ANALYTICS DETAILS 013
I3853 - ANALYTICS DETAILS 014
I3854 - ANALYTICS DETAILS 015
Filter
Analytic details
-

These alarms have been defined as IntrusionTrace alarms:

- Camera 1: I3840–I3855
- Camera 2: I3856–I3871
- Camera 3: I3872–I3887
- Camera 4: I3888–I3903
- Camera 5: I3904–I3919
- Camera 6: I3920–I3935
- Camera 7: I3936–I3951
- Camera 8: I3952–I3967
- Camera 9: I3968–I3983
- Camera 10: I3984–I3999
- Camera 11: I4000–I4015
- Camera 12: I4016–I4031
- Camera 13: I4032–I4047
- Camera 14: I4048–I4063
- Camera 15: I4064–I4079
- Camera 16: I4080–I4095

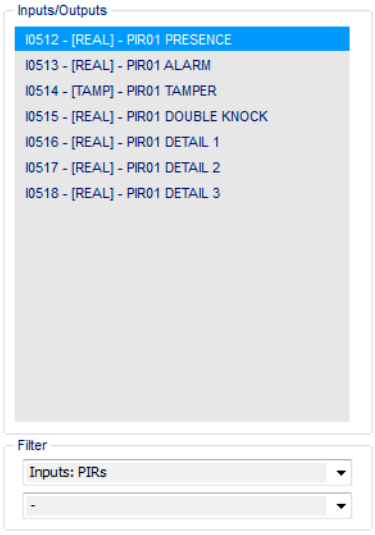
These alarms can be added to a detection area in the IntrusionTrace configuration window.



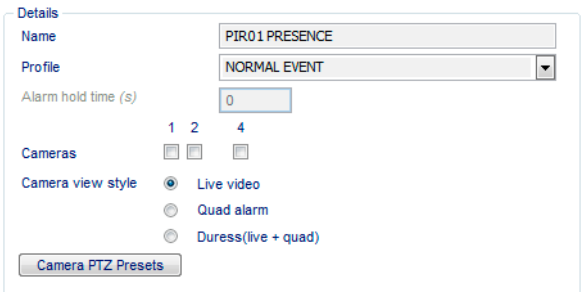
13.5 PIR Alarms

From version 2.06.0020, extra PIR alarms for ADPRO PIR detectors have been added. These alarms provide more detailed information on the indicated alarms. It is important that the server knows the type of the connected ADPRO PIR detector, because depending on the type of detector other alarms will be issued. The RMG should be able to automatically detect the type of ADPRO PIR detector.

See also *Connecting the PIRs* on page 128.


Inputs/Outputs
I0512 - [REAL] - PIR01 PRESENCE
I0513 - [REAL] - PIR01 ALARM
I0514 - [TAMP] - PIR01 TAMPER
I0515 - [REAL] - PIR01 DOUBLE KNOCK
I0516 - [REAL] - PIR01 DETAIL 1
I0517 - [REAL] - PIR01 DETAIL 2
I0518 - [REAL] - PIR01 DETAIL 3
Filter
Inputs: PIRs
-

All alarms have by default been assigned to the normal event profile.



8 alarms per PIR detector have been defined as PIR alarms:

	Presence	Alarm	Tamper	Double Knock	Detail 1	Detail 2	Detail 3	Reserved
PIR 1	I512	I513	I514	I515	I516	I517	I518	I519
PIR 2	I520	I521	I522	I523	I524	I525	I526	I527
PIR 3	I528	I529	I530	I531	I532	I533	I534	I535
PIR 4	I536	I537	I538	I539	I540	I541	I542	I543
PIR 5	I544	I545	I546	I547	I548	I549	I550	I551
PIR 6	I552	I553	I554	I555	I556	I557	I558	I559
PIR 7	I560	I561	I562	I563	I564	I565	I566	I567
PIR 8	I568	I569	I570	I571	I572	I573	I574	I575
PIR 9	I576	I577	I578	I579	I580	I581	I582	I583
PIR 10	I584	I585	I586	I587	I588	I589	I590	I591
PIR 11	I592	I593	I594	I595	I596	I597	I598	I599

	Presence	Alarm	Tamper	Double Knock	Detail 1	Detail 2	Detail 3	Reserved
PIR 12	I600	I601	I602	I603	I604	I605	I606	I607
PIR 13	I608	I609	I610	I611	I612	I613	I614	I615
PIR 14	I616	I617	I618	I619	I620	I621	I622	I623
PIR 15	I624	I625	I626	I627	I628	I629	I630	I631
PIR 16	I632	I633	I634	I635	I636	I637	I638	I639
PIR 17	I640	I641	I642	I643	I644	I645	I646	I647
PIR 18	I648	I649	I650	I651	I652	I653	I654	I655
PIR 19	I656	I657	I658	I659	I660	I661	I662	I663
PIR 20	I664	I665	I666	I667	I668	I669	I670	I671
PIR 21	I672	I673	I674	I675	I676	I677	I678	I679
PIR 22	I680	I681	I682	I683	I684	I685	I686	I687
PIR 23	I688	I689	I690	I691	I692	I693	I694	I695
PIR 24	I696	I697	I698	I699	I700	I701	I702	I703
PIR 25	I704	I705	I706	I707	I708	I709	I710	I711
PIR 26	I712	I713	I714	I715	I716	I717	I718	I719
PIR 27	I720	I721	I722	I723	I724	I725	I726	I727
PIR 28	I728	I729	I730	I731	I732	I733	I734	I735
PIR 29	I736	I737	I738	I739	I740	I741	I742	I743
PIR 30	I744	I745	I746	I747	I748	I749	I750	I751
PIR 31	I752	I753	I754	I755	I756	I757	I758	I759
PIR 32	I760	I761	I762	I763	I764	I765	I766	I767

The meaning of the details alarms differ according to the type of detector:

Detector type	Detail 1 (alarm type)	Detail 2 (alarm type)	Detail 3 (alarm type)
PRO 45Z	IR (infrared)	–	–
PRO 45 / PRO-E 45			
PRO 45H / PRO-E 45H			
PRO 18W / PRO-E 18W			
PRO 18WH / PRO-E 18WH			
PRO 18 / PRO-E 18			
PRO 18H / PRO-E 18H			
PRO 40 / PRO-E 40			
PRO 30 / PRO-E 30			
PRO 45D	Right	Left	–
PRO 45DH			
PRO 100 / PRO-E 100	Short range	Medium range	Long range
PRO 100H / PRO-E 100H			
PRO 250H			

Detector type	Detail 1 (alarm type)	Detail 2 (alarm type)	Detail 3 (alarm type)
PRO 50 / PRO-E 50	Left	Centre	Right
PRO 85 / PRO-E 85			
PRO 85H / PRO-E 85H			

13.6 Arm/Disarm Switch

Events on the server can be classified in the following groups:

- system messages: these are internal events (e.g. hard disk error, power supply fault, communication error…);
- camera messages (e.g. video signal missing, contrast level too low, motion detected…);
- network inputs: alarm inputs connected to external Net I/O modules
- inputs: alarm inputs connected to the OTB I/O card, accessible at the back of the video system;
- virtual inputs: events detected on interconnected S3100 security panels.
- workbits: calculated bits that provide alarm information. A combination of inputs can trigger a workbit.

Events have to be handled in a different way when the building is left unattended. Therefore, the building has to be armed. Arming can be done in three ways:

1. automatically according to a schedule;
2. manually, by a user who has to activate a switch;
3. by the CMS, executing the DN command line in Telnet (hint: type HE for syntax help).

To define the behaviour of an alarm input during armed and disarmed state, modify the alarm profile that is assigned to this input.

Note

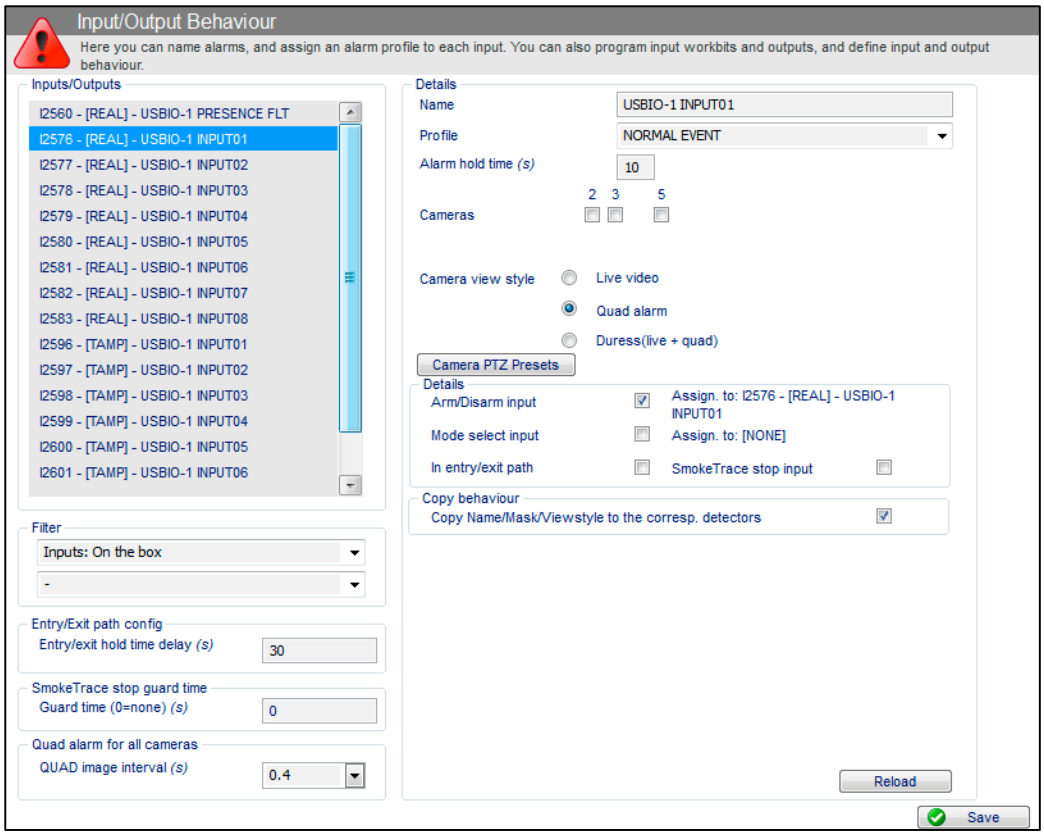
It is possible for other software developers to use the SDK (software development kit) in order to arm/disarm a building.

To define an arm/disarm switch, open **System > Behaviour > Input/output behaviour**. Select an input from the list.

Note

You can use only real inputs (USB I/O), network inputs (Net I/O), or workbit inputs.

Apply a filter to reduce the list.



Select the **Arm/Disarm input** check box; modify the settings if necessary, and click **Save** to apply the new settings.

13.7 Activating Outputs

To activate an output, open the *Input/Output Behaviour* window via **System > Behaviour > Input/Output Behaviour**.

Select an output from one of these groups:

- On the box: outputs on the OTB I/O cards, 8 outputs on the first set (MIO and EIO cards) and 8 outputs on the second set.
- Network: outputs available on the Net I/O modules, connected to the Ethernet.
- VM22A: an output that activates the corresponding loudspeaker on the VM22A audio.
- Workbits: virtual outputs that can be used to store internal states.

Inputs/Outputs
C2560 - [OUTP] - USBIO-1 GREEN LED
C2561 - [OUTP] - USBIO-1 YELLOW LED
C2562 - [OUTP] - USBIO-1 DISC LED
C2563 - [OUTP] - USBIO-1 BUZZER
C2576 - [OUTP] - USBIO-1 OUTPUT01
C2577 - [OUTP] - USBIO-1 OUTPUT02
C2578 - [OUTP] - USBIO-1 OUTPUT03
C2579 - [OUTP] - USBIO-1 OUTPUT04
Filter
Outputs: On the box
-

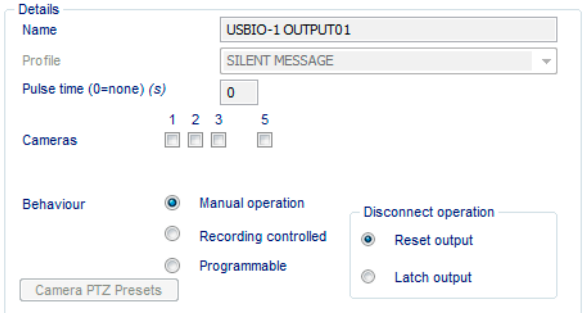
Apply a filter to reduce the list.

Click **Save** to apply the new settings.

> ***Note***
>
> Outputs that are already used for another operation cannot be modified here.

13.7.1 Manual Operation

Select the desired output and choose *Manual operation*.



The output will thus need to be switched by a user from the client software.

To allow the specific output to be activated from the **Live Video** window, select the cameras on which this ***activate output*** button has to appear.

For more information, see *Activating an Output Manually* on page 149.

You also have to define which action needs to be taken when closing the client software application:

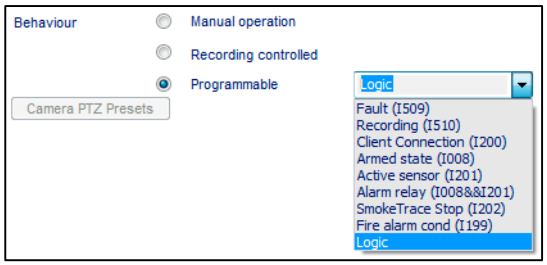
- Reset output: the output always resets to idle state when closing the client application.
- Latch output: the output remains in the selected state, even after closing the client application.

13.7.2 Recording Controlled

If you set an output to **Recording controlled**, that output can be activated when a recording is started. See *Cameras* on page 67.

13.7.3 Programmable Output

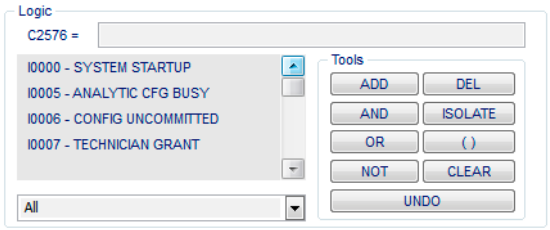
This option activates an output in function of a condition or event. The condition is specified in the drop-down list:



With the last option –*Logic*– you can define a specific condition, selecting particular inputs linked with **AND** and **OR** functions. Brackets allow to modify the order of evaluation (which is normally from left to right). The state of an input can be inverted (**NOT** function) and the isolate state of an alarm can be selected (**ISOLATE**). Select an input from the list and click **ADD** (in the *Tools* section) to insert it at the current position. On error, click **DEL**. To clear the whole line, click **CLEAR**.

Click the **NOT** button before adding an input if you want to invert its state.

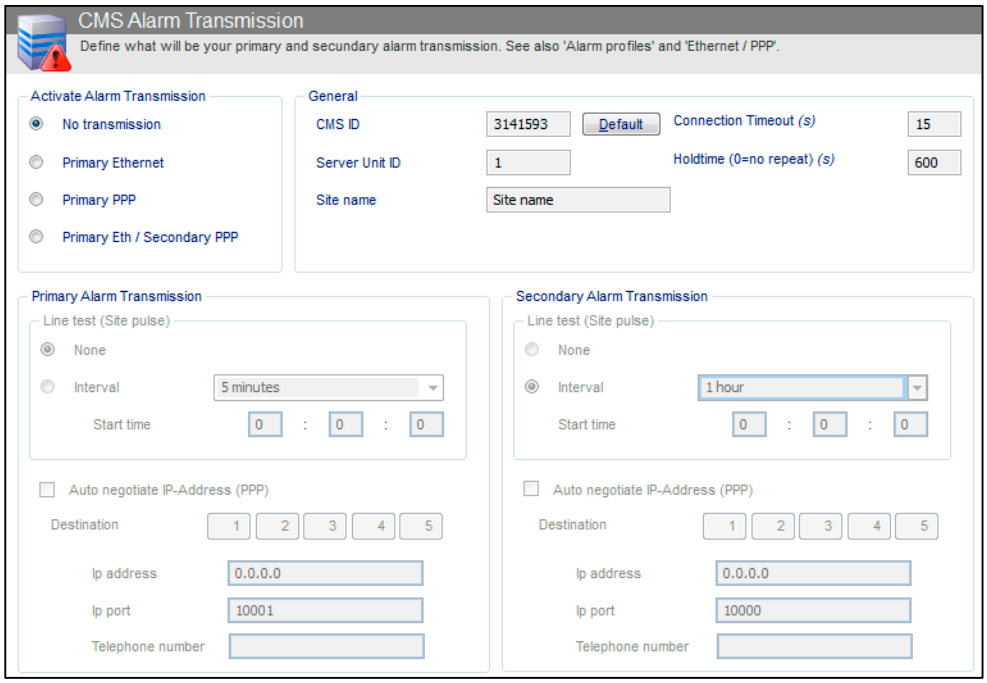
Click the **ISOLATE** button just after adding an input if you want to read its operational state (isolated or not). The letter M appears in front of the number of the selected input.



Example: I2144 AND I2145 OR M2146 AND NOT I2145.

14 Alarm Transmission

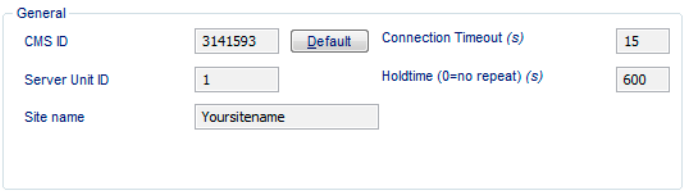
To activate alarm transmission through main channel and/or backup channel, open **System > Behaviour > Alarm Transmission > CMS Alarm Transmission**. Modify the settings and click **Save**.



Choose which kind of alarm transmission has to be configured:

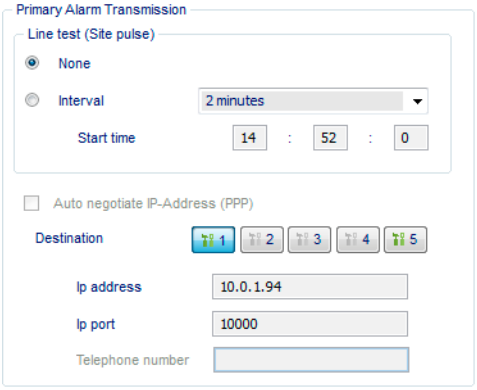
Parameter	Description	Default value
Activate Alarm Transmission	• No transmission; • Primary Ethernet: the video server connects to the CMS through a LAN connection; • Primary PPP: the video server connects to the CMS through a dial-up connection (requires an external modem connected to USB port /dev/ttyU1); • Primary Eth / Secondary PPP: the video server connects to the CMS through a LAN as main connection and a dial-up network as backup connection. The backup connection is used when transmission on the main connection is unsuccessful.	No transmission

14.1 General



Parameter	Description	Default value
CMS ID	Sender signature (this number has to match the number programmed in the alarm management software)	3141593
Server Unit ID	Site identification number (1–9999). This number has to be unique for each video system that sends alarms to the same computer.	1
Site name	Name of the site. This information is required if connecting to Central Video software. The site name can also be displayed on the camera images.	Site name
Connection timeout (s)	Disconnects automatically if no more data is exchanged for the specified time duration.	15 (seconds)
Hold time (0 = no repeat) (s)	This specifies a delay, expressed in seconds, before re-attempting to connect, when a connection error occurred. If “0”, the system will not try again (= only recommended if a backup connection is available).	600 (seconds)

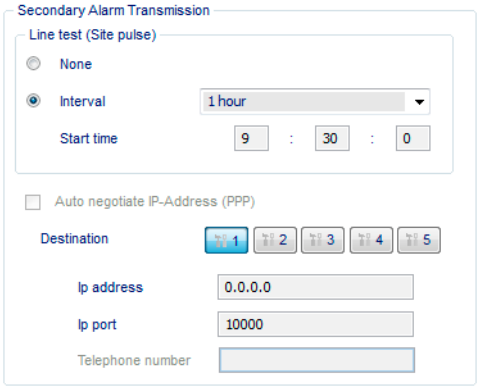
14.2 Primary Alarm Transmission Settings



Parameter	Description	Default value
Line test	• None; • Interval: this will send a life check message every x minutes. To make sure this functions correctly, the message (I0034 – [SYST] – Primary lifecheck) needs to be configured with a correct alarm profile! Also set the time on which the first alarm transmission should be sent. ***Note*** For dial-up networks it is recommended to execute the line test less frequently, because of the connection cost (e.g. 1 test a day).	None

Parameter	Description	Default value
Destination	You can enter the parameters for 5 different computers that will receive alarms. Click the number you would like to define (or see). ***Note*** The alarm will only be sent to 1 IP address. Only when no communication with the first IP address can be established, the second IP address will be used. If still no communication is possible, the third, fourth, and fifth IP address will be used. If none of the 5 defined IP addresses are available, the backup transmission will be activated. Alarm reception requires appropriate alarm management software on the computer (e.g. VCP, EMS, or M3000).	
IP address	Enter the IP address of the computer that will receive alarms.	0.0.0.0
IP port	Enter the IP port on which alarms must be transmitted.	10000
Telephone number	Enter the telephone number to which alarms must be transmitted. This option is only available for a dial-up network.	–

14.3 Secondary Alarm Transmission Settings



Parameter	Description	Default value
Line test	• None; • Interval: this will send a life check message every x minutes. To make sure this functions correctly, the message (I0035 – [SYST] – Backup lifecheck) needs to be configured with a correct alarm profile! Also set the time on which the first alarm transmission should be sent. ***Note*** For dial-up networks it is recommended to execute the line test less frequently, because of the connection cost (e.g. 1 test a day).	None
Auto-negotiate IP address (PPP)	This option is only available for a dial-up network. When ticked, IP addresses will be assigned by the CMS, during the time of the communication. This option is required if the CMS uses the Video Central Platinum software.	Not selected

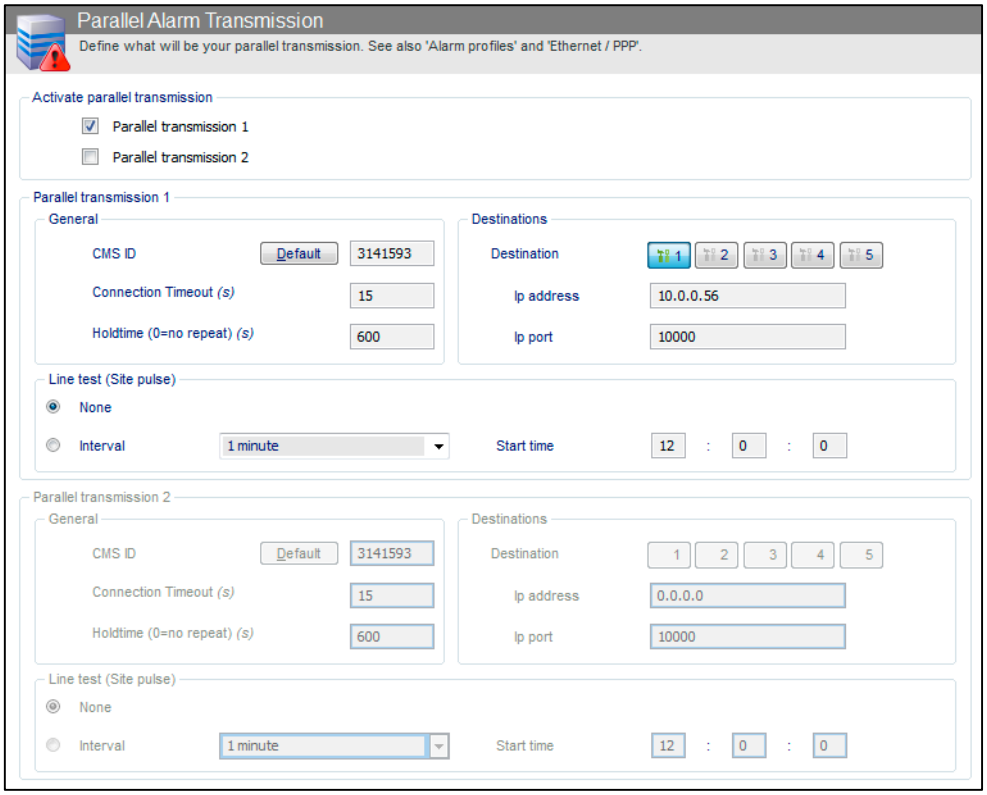
Parameter	Description	Default value
Destination	You can enter the parameters for 5 different computers that will receive alarms. Click the number you would like to define (or see). ***Note*** The alarm will only be sent to 1 IP address. Only when no communication with the first IP address can be established, the second IP address will be used. If still no communication is possible, the third, fourth, and fifth IP address will be used. If none of the 5 defined IP addresses are available, the backup transmission will be activated. Alarm reception requires appropriate alarm management software on the computer (e.g. VCP, EMS, or M3000).	
IP address	Enter the IP address of the computer that will receive alarms.	0.0.0.0
IP port	Enter the IP port on which alarms must be transmitted.	10000
Telephone number	Enter the telephone number to which alarms must be transmitted. This option is only available for a dial-up network.	–

14.4 Setting up Parallel Transmission

Besides the transmission to the main CMS, you can set up parallel transmission to two more monitoring stations.

To set up parallel transmission, proceed as follows:

1. Choose **System > Behaviour > Alarm Transmission > Parallel Alarm Transmission**.



2. To activate parallel transmission, select the check boxes for **Parallel transmission 1** and/or **2**.
3. Provide the required settings for each parallel transmission channel. Setup is similar to that of the primary transmission. For more information, see *General* on page 118; and also *Primary Alarm Transmission Settings* on page 119.

4. When finished, click **Save** to confirm.

15 Analytics

When you have activated specific application licenses – like IntrusionTrace and LoiterTrace – you will see this reflected in the menu. If not activated, these applications will not be visible in the menu tree.

15.1 The Xtralis Xapps

- IntrusionTrace
  For more information on the IntrusionTrace application, see the IntrusionTrace documentation.
- LoiterTrace
  For more information on the LoiterTrace application, see the LoiterTrace documentation.
- SmokeTrace
  For more information on this application, see the SmokeTrace documentation.
- ClientTrace
  For more information on the ClientTrace application, see the ClientTrace documentation.

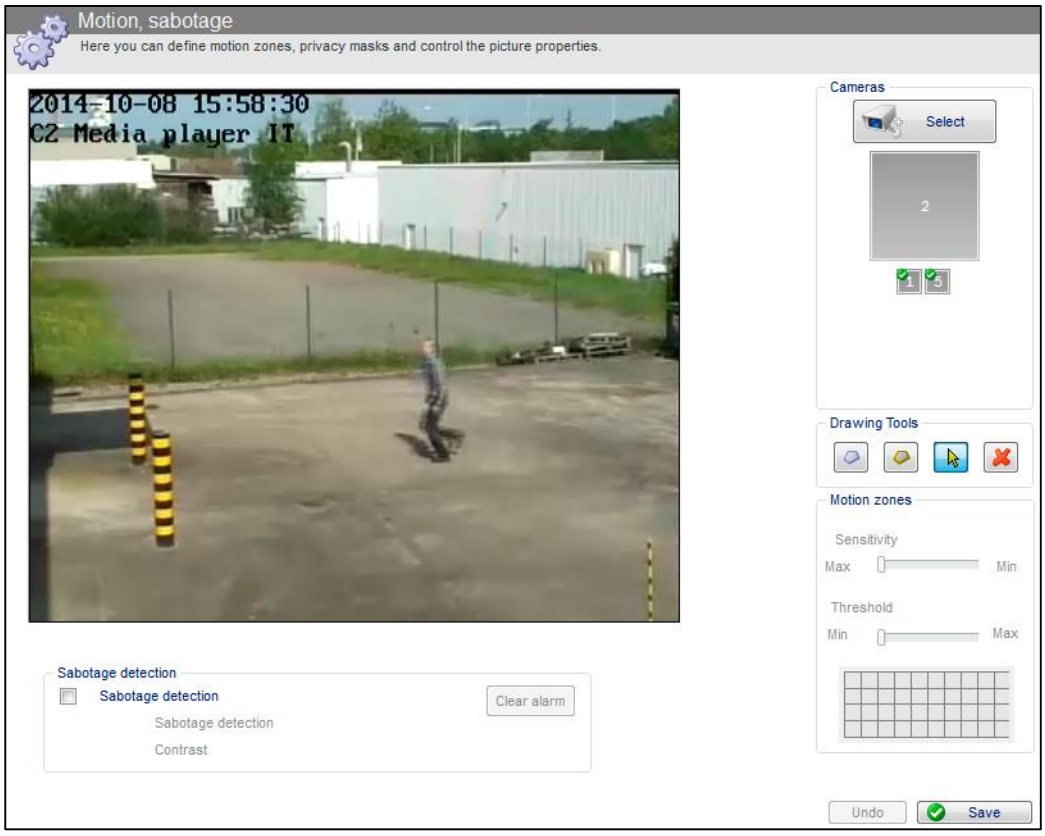
15.2 Motion, Sabotage

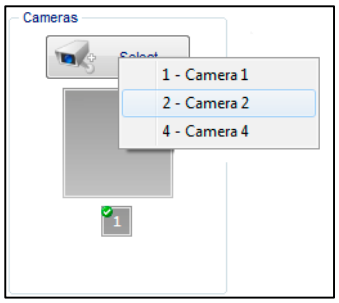
15.2.1 Motion, Sabotage Interface

Open the *Motion, sabotage* window via System > Behaviour > Analytics > Motion, sabotage.

15.2.2 Cameras

Click the **Select** button and click the camera you would like to configure. The live image will appear.





15.2.3 Drawing Tools

Button	Description
	Define a detection zone. A maximum of 4 detection zones can be defined. These zones can overlap. For more information, see *Motion Detection Zones* on page 124.
	Define a private zone. A maximum of 4 private zones can be defined. These zones can overlap. For more information, see *Private Zones* on page 125.
	Click an object to select it.
	Delete the selected object.

15.2.4 Motion Detection Zones

Per camera up to 4 motion detection fields can be defined. Detection of a moving object within this field will trigger an alarm that can be transmitted to the CMS. Motion detection can also be used to start a new recording.

In *Drawing Tools* click the button with the blue polygon.

A blue square appears on the video image. The square also gets a number (1 to 4). You can adjust the size and position of the shape by clicking the form with the left mouse button.

When you select (= click) the blue square, the colour changes to orange. Now you can adapt the motion detection settings.

You can adjust the size and position of the detection zone. Define the motion zone settings in the section *Motion zones*. For more information, see *Motion Zone Detection Settings* on page 126.

15.2.5 Private Zones

> ***Note***
>
> It is not possible to draw private zones if the camera has PTZ enabled.

Outdoor security cameras may unintentionally look into neighbourhood residences. To respect their privacy, these parts of the picture can be masked.

Click the button with the yellow polygon in *Drawing Tools*.

A yellow striped black square will appear in the left upper corner of the image.

You can adjust the size and position of the rectangle to make sure the correct zone is masked. A black rectangle will appear on the image, which will also be shown in the live image.

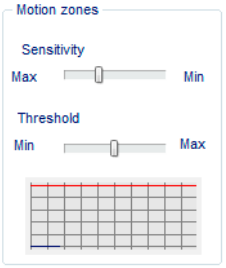
Up to 4 zones can be masked.

15.2.6 Motion Zone Detection Settings

The detection settings depend on the type of camera that you use: analogue or IP.

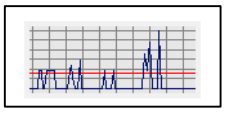
For analogue cameras you can adjust the sensitivity and the threshold for each detection zone.

- **Sensitivity**: specifies how much the luminance of the pixels in the zone has to change to detect motion.
- **Threshold**: sets the number of pixels in the zone that have to change in order to detect motion. This defines the size of the objects that you can detect. With a large threshold, only large objects will trigger motion detection.



It takes some testing to find the optimal settings. Some guidelines for successful motion detection with analogue cameras:

- Use uniform lighting.
- Switch off AGC (automatic gain control) in the camera.
- Keep the sensitivity as low as possible. If sensitivity is high, small illumination changes may cause false alarms.
- Keep the detection zones as small and narrow as possible. With large detection zones, you have to increase the sensitivity in order to detect motion. This in turn may increase the number of false alarms. Also, relatively small objects may not be detected in a large zone.
- Use the graph to test the settings for each zone. Click a zone to select it, and the detection level in that zone appears in the graph. The horizontal red line indicates the threshold. The detection level (black line) must exceed the threshold to trigger motion detection.

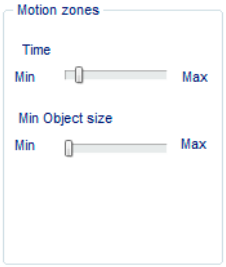


Note

To get a feel for how the different settings influence detection, adjust only one setting at a time: sensitivity, threshold, or the size and shape of the detection zone.

For IP cameras you can adjust time and minimum object size for each detection zone:

- **Time**: sets the detection delay. Minimal delay means that the motion is detected immediately when an object starts moving in the detection zone. Maximal delay means that the motion is detected when the object is moving inside the detection zone for some time.
- **Min Object size**: sets the object size relative to the region size. Minimal object size means that even very small objects (such as small animals like cats and dogs) will trigger motion detection. Maximal object size means that only very large objects will trigger motion detection.



It is recommended to test out the settings to obtain the best result.

When motion is detected in the detection zone, the border of the zone turns red.

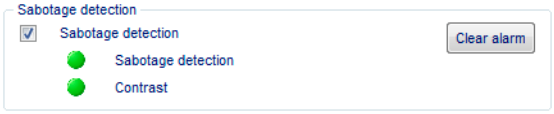
Click **Save** to apply the new settings.

To remove a motion detection zone, select the detection zone and click **Remove**.

Click **Save** to apply the new settings.

15.2.7 Sabotage Detection

When a device is being tampered with, the sabotage detection will generate a so-called tamper alarm. This can be activated per camera. In order to do so, tick the option in the section *Sabotage detection*.



The following actions with the camera will result in a tamper alarm:

- the lens is covered
- the position of the camera is altered
- the zoom of the camera image is changed
- the focus of the camera image is changed

When a tamper alarm is being generated on a certain camera, the green colour for status will change to red. The tamper alarm on the camera should be cleared manually. To clear the tamper alarm on the camera, click **Clear alarm**.

Click **Save** to apply the new settings.

16 PIR Settings

16.1 Required PIR Firmware

For a correct functioning of the PIR alarm processing, a minimal PIR firmware version 2.00 is required. Previous firmware versions also work with RS-485 communication, but do not support all features (e.g. Alarm Management).

16.2 Connecting the PIRs

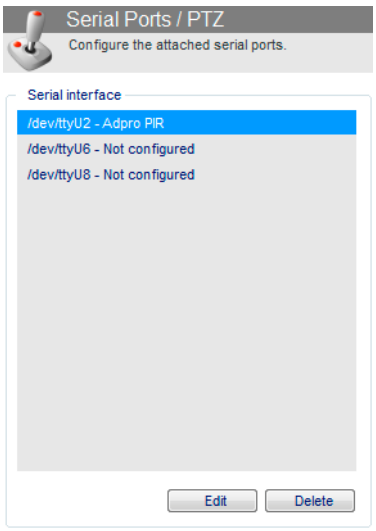
For physically connecting the PIRs to the server, see the *FastTrace 2 Hardware Installation Manual*.

> ***Note***
>
> From firmware version 2.6 onwards, a separate PIR-HLI application license is required to configure the PIR devices. For more information, see *Application Licenses* on page 154.

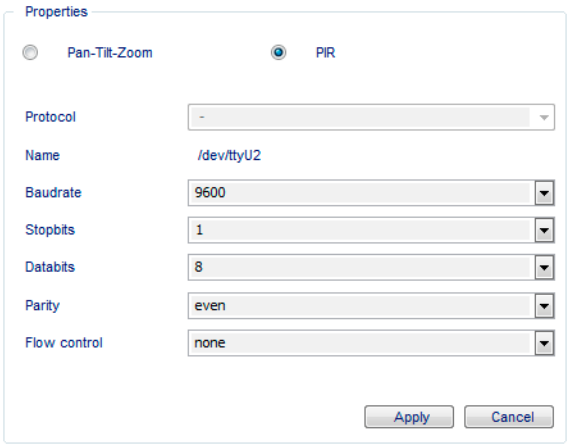
16.3 Configuring the Software Settings

16.3.1 Configuring the Serial Port

You need to set the serial port to PIR. Open the *Serial Ports / PTZ* window via **System > Connections > Serial Ports / PTZ**.



Select the desired serial interface from the list and click **Edit**. The *Properties* section will appear to the right.



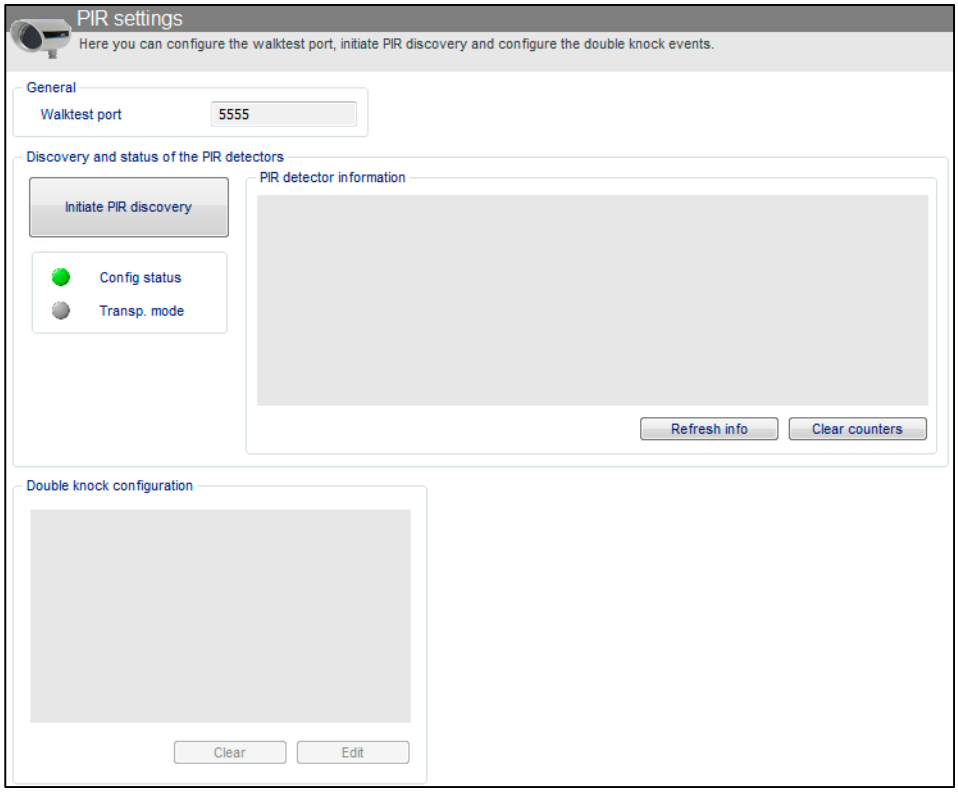
Choose the *PIR* option. By default all parameters are attributed. There is no need to change any of the settings.

Note

- When using the USB to RS485 distribution unit or the USB to serial port RS485 converter, your only option is to use the /dev/ttyU2 USB port.
- When connecting your PIR directly to the Main I/O of the server (using an RS-485 cable), you will have to use either the /dev/ttyU6 USB port (for the first Main I/O card) or the /dev/ttyU8 USB port (for the second Main I/O card). These ports are automatically detected by the XOa client software.

16.3.2 Initiating the PIR Discovery

Open the PIR settings window via **System > Behaviour > PIR settings**.



16.3.2.1 General

In this section you can set the walk test port. This port is used for the iPIR app. This app allows you to configure your PIR settings and visualize PIR detections on a scope on your mobile device. For more information, see the *iPIR User Manual*. For iPIR to work, you have to enable Technician access. See *Granting the Technician* on page 140.

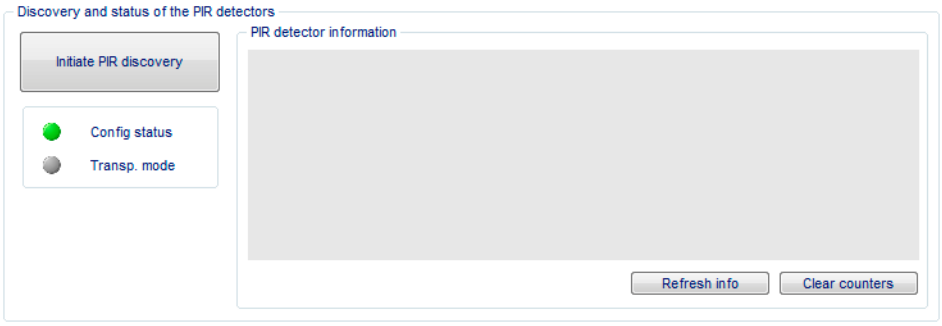
The default walk test port to use with iPIR is 5555.

16.3.2.2 Discovery and Status of the PIR Detectors

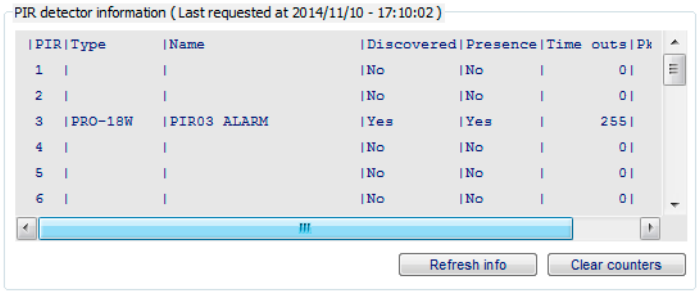
The **Discovery and status of the PIR detectors** panel displays the connected PIR devices and their status.

If the PIR devices are operating normally, a green circle appears for **Config status**. The circle turns yellow when there is a problem with configuration of one of the PIR devices (for example if the serial port is not configured correctly).

During PIR commissioning, while the walk test port is in use (for example by the iPIR app), the transparent mode (**Transp. Mode**) is active. In transparent mode, the RMG does not transmit alarms/events from the PIR devices to the CMS. This allows for testing and adjusting the PIR devices before going 'live'.



Click **Initiate PIR discovery** to search the server for any connected PIR devices. The **PIR detector information** panel displays the found PIR devices:


PIR detector information (Last requested at 2014/11/10 - 17:10:02)
|PIR|Type |Name |Discovered|Presence|Time outs|Pk
1 | | |No |No | 0|
2 | | |No |No | 0|
3 |PRO-18W |PIR03 ALARM |Yes |Yes | 255|
4 | | |No |No | 0|
5 | | |No |No | 0|
6 | | |No |No | 0|
Refresh info
Clear counters

Click **Refresh info** to search for connected PIR devices again.

Click **Clear counters** to reset the numbers in the **Time outs** and **Pkt Errors** columns.

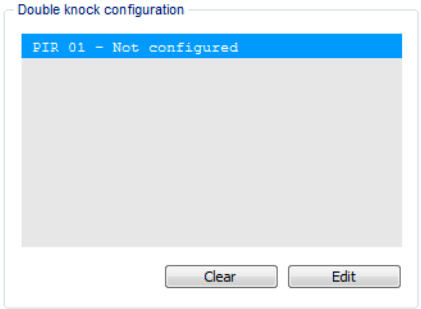
16.4 Double-Knock Configuration

To reduce the number of false alarms from a PIR, you can use double-knock configuration. In a double-knock configuration, the double-knock event is only triggered when another trigger occurs simultaneously. Typically, you combine the PIR with a camera for analytics.

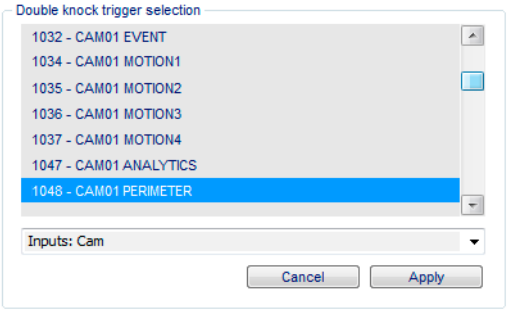
> ***Note***
>
> You need to set up the correct alarm profile for the double-knock input so that it transmits the alarm, and you need to set up the individual inputs so that they do not transmit alarms. For an overview of the PIR alarm inputs, see *PIR Alarms* on page 112.

To set up a PIR in a double-knock configuration, proceed as follows:

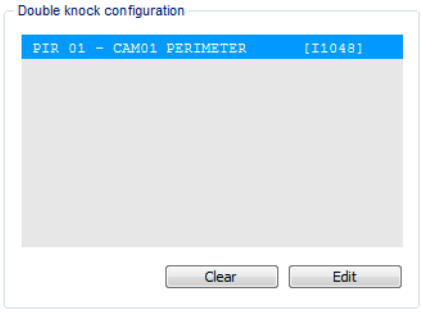
1. Choose **System > Behaviour > PIR Settings**, and click **Initiate PIR Discovery**. The available PIR devices appear in the **Double knock configuration** list.



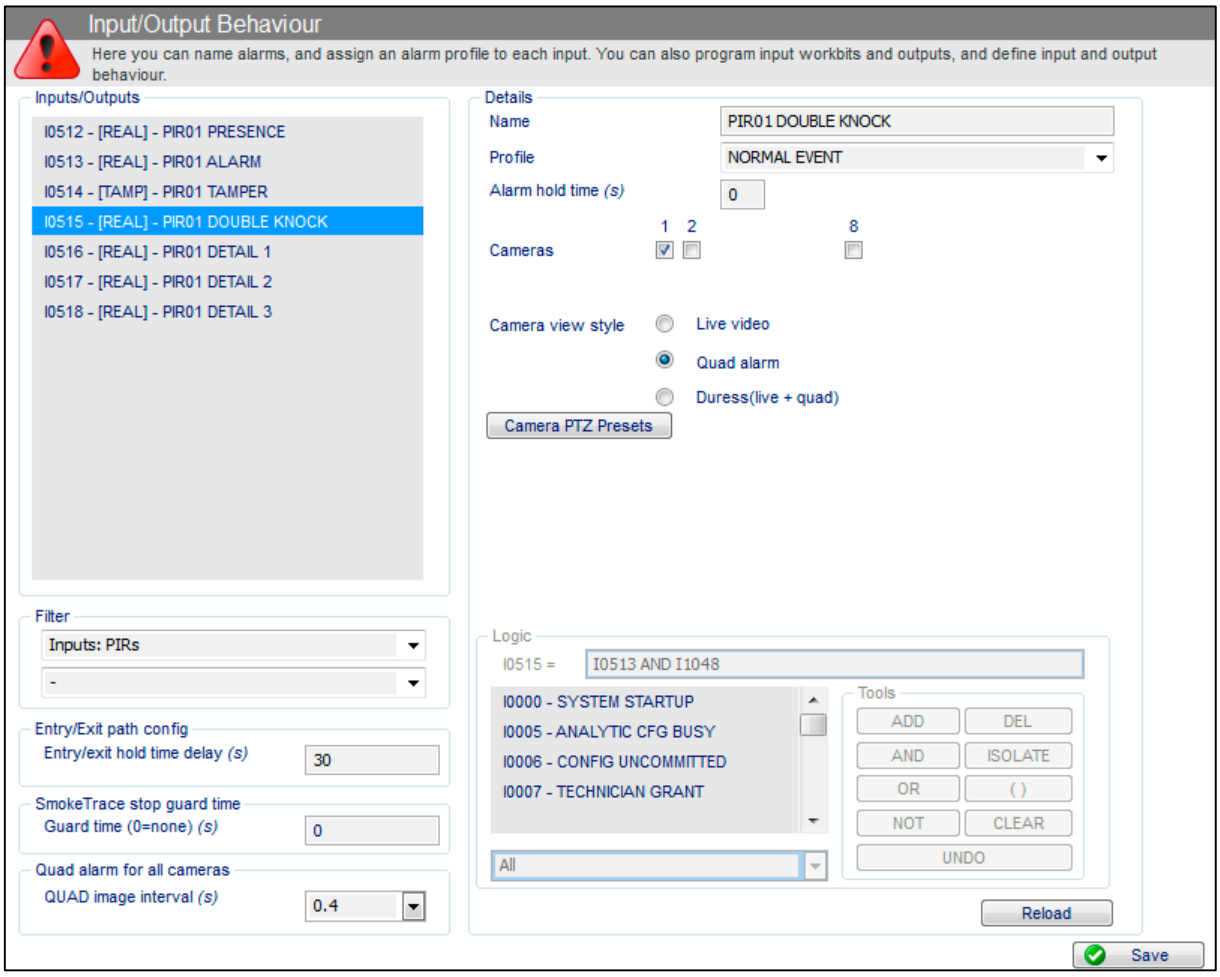
2. Select the PIR that you want to configure, and then click **Edit**. The list of available triggers appears.
3. If necessary, filter the list (for example on camera inputs), and then click the desired trigger. In the example below, the IntrusionTrace alarm on camera 01 is selected.



4. Click **Apply**. The selected trigger appears in the **Double knock configuration** list.



5. Click **Save** to save the PIR settings.
   Now you can set up the desired alarm profile for the double-knock input.
6. Click **Input/Output Behaviour**.
7. In the **Inputs/Outputs** list, select the PIR's double-knock input (I0515 in the example). Use the **Inputs: PIRs** filter to reduce the list of inputs/outputs.



> ***Note***
>
> Under **Logic**, the following logical function appears (not editable):
> I0515 = I0513 AND I1048
> This means that the double-knock input (I0515) is activated if the normal PIR event (I0513) AND the camera event (I1048) are active.

8. In the **Profile** box, select the desired alarm profile for the double-knock alarm.
   Now you can set up the individual inputs so that they do not transmit alarms.
9. Select the normal PIR event (I0513 in the example) and set the alarm profile to SILENT MESSAGE.
10. Select each of the PIR detail events (I0516–I0518 in the example), and set the alarm profile to SILENT MESSAGE.
11. Select the camera event (I1048 in the example) and set the alarm profile to SILENT MESSAGE.
12. Click **Save**.

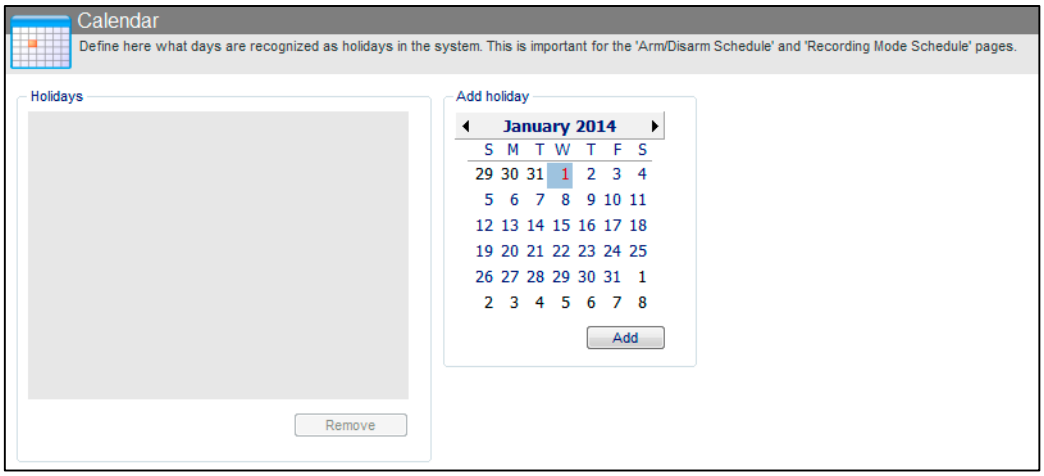
17 Calendar

The holiday calendar lets you control the behaviour of the video system during holidays. It affects:

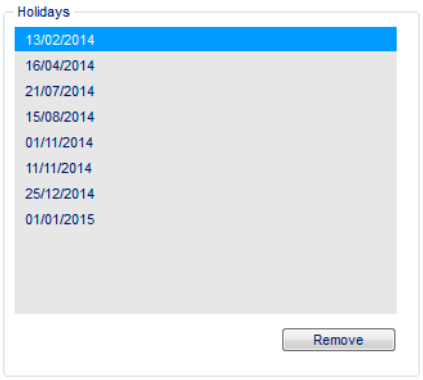
- Your video recorders
- The operational mode of the video system (if managed by a mode schedule)
- The arm/disarm schedule.

To set up the holiday calendar, proceed as follows:

1. Choose **System > General > Calendar**.


Calendar
Define here what days are recognized as holidays in the system. This is important for the 'Arm/Disarm Schedule' and 'Recording Mode Schedule' pages.
Holidays
Remove
Add holiday
January 2014
S M T W T F S
29 30 31 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31 1
2 3 4 5 6 7 8
Add

2. To set a day as a holiday, select the date in the **Add holiday** box, and then click **Add**. The holiday appears in **Holidays** list.



3. Repeat for each holiday.
4. To remove a day, click the date in the Holidays list, and then click **Remove**.
5. Click **Save**.

It is recommended to clean up the holiday list once per year. Although there is no need to delete holidays that have passed, it will help you keep an overview.

18 Users

18.1 About Users

In versions before XOa 3, it was possible to have two or more users with the same username (for example Administrator). Also, it was possible to have usernames that contain only digits.

As of version XOa 3, usernames must be alphanumeric (= must contain at least one letter), and each username must be unique.

The following user types exist, each with different access rights:

- Administrator: has full access rights.
- User: has specific rights, adjustable per user.
- Technician: has specific rights, adjustable per user. Technicians can only log on if an Administrator or another user has granted them access.

You can create up to 32 users. The following default users are pre-defined:

User ID	Username	Password	User Type
0	Administrator	666777	Administrator
1	Administrator1	666777	Administrator
15	Technician	666777	Technician

For security reasons, it is strongly recommended to change the passwords of the default users. See *Modifying or Deleting an Existing User* on page 139.

18.2 About Strong Passwords

To increase security, you can choose to use strong passwords. Strong passwords have to meet minimum requirements:

- The password has to contain at least 8 characters.
- The password has to contain at least 1 capital letter and at least 1 small letter.
- The password has to contain at least 1 digit.

Examples of strong passwords are:

- Tmus001cl
- 12rtSV5km
- aiGP5rsLZa89

Furthermore, you can set an expiry time (in days) for the password. The user then has to change the password before it expires. Finally, you can limit the number of retries to log on. When the user has reached the maximum number of retries, the system temporarily blocks the user account. You specify how long (in seconds) the user account is blocked.

The default values of strong passwords are:

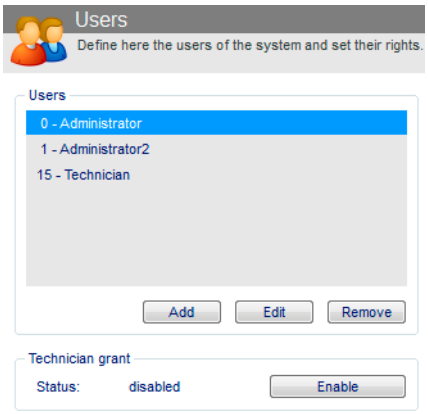
Parameter	Unit	Range	Default value
Maximum password age	Days	0–120	0 (= not applicable)
Nr of invalid login attempts	–	0–10	3
Nr of seconds user is blocked	Seconds	0–3600	60

18.3 Adding New Users

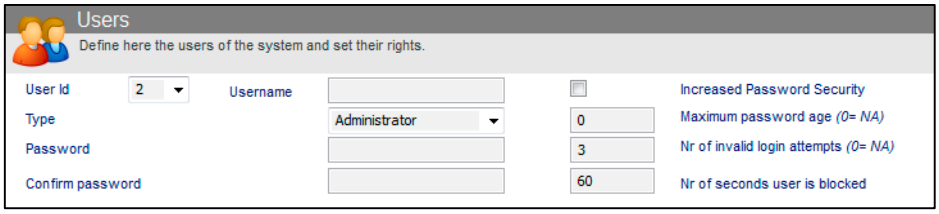
Only Administrator users can add or delete users.

To add a user, proceed as follows:

1. Choose **System > General > Users**.



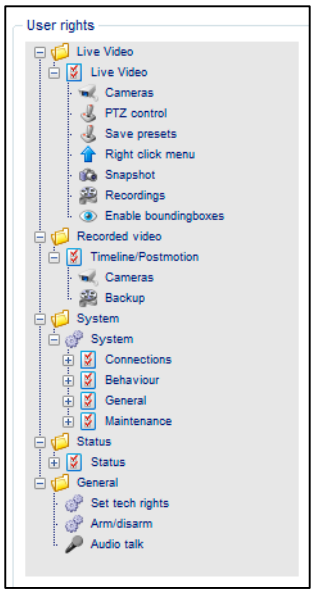
2. Click **Add**.



3. Provide the following information:
   - **User Id**: select a user ID.
   - **Username**: type a username. The username must be unique and contain at least one letter.
   - **Type**: select the desired user type (Administrator, User, or Technician).
   - **Increased password security**: select the check box if you want to use strong passwords.
   - **Maximum password age (0 = NA)**: type the number of days (0–120) after which the password expires. Type 0 if you don't want the password to expire.
   - **Nr of invalid login attempts (0 = NA)**: type the number of times (0–10) a user can enter an incorrect username/password before the system blocks the user. Type 0 if you do not want to restrict the number of logon attempts.
   - **Password**: type a password for the user.
   - **Confirm password**: type the password again.
4. If you have selected user type User or Technician, you have to set the access rights. By default, all rights are selected. For details, see *User Rights* on page 135.
5. Click **Apply**.
6. Click **Save**.

18.4 User Rights

For users of type User or Technician, you need to specify the rights of the individual user. If you select one of these user types, the access rights panel appears:



Note

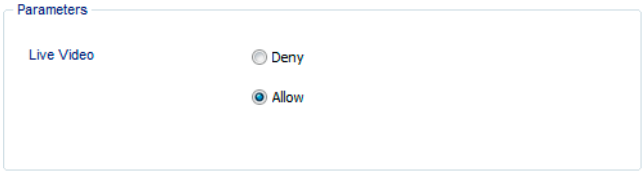
If you want to tick all options (rights), you can click **Set all**.

If you want to clear all options (rights), you can click **Clear all**. All options will be cleared, but the user itself will not be deleted!

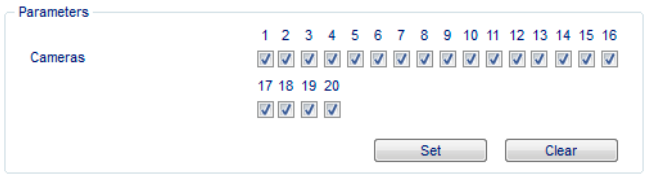
18.4.1 Live Video

Define whether or not the specific user can access the **Live Video** window in the XOa client. Proceed as follows:

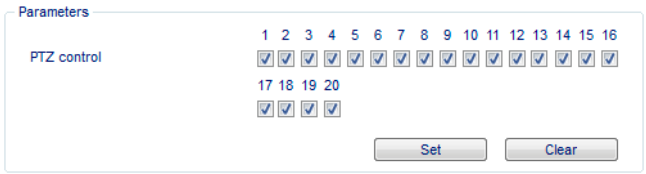
1. In the access rights panel, choose **Live Video > Live Video**.



2. Click **Deny** if you do not want the user to access the **Live Video** window. In this case, you can skip all following steps. If you allow the user to access the **Live Video** window, continue with the setup.
3. To define which cameras the user can view, click **Cameras**. By default all cameras are selected.

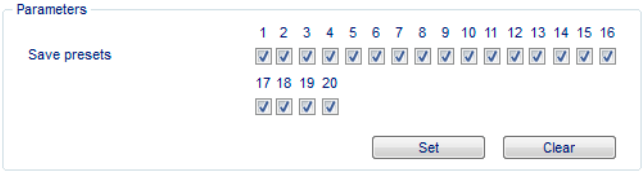


4. Clear the check boxes for the cameras that this user is not allowed to view, and click **Set**.
   You can click **Clear** to clear all the check boxes, and then select just the few cameras that are allowed.
5. To define for which cameras the user can control PTZ, click **PTZ control**.



6. Clear the check boxes for the cameras for which this user is not allowed to use PTZ control, and click **Set**.
   You can click **Clear** to clear all the check boxes, and then select just the few cameras that are allowed.

7. To define for which cameras the user is allowed to save PTZ presets, click **Save presets**.



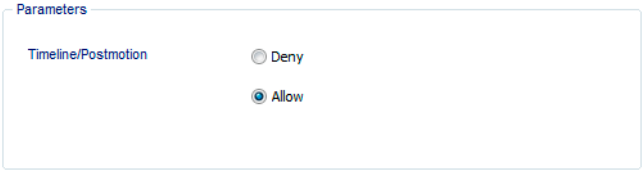
8. Clear the check boxes for the cameras for which this user is not allowed to save PTZ presets, and click **Set**.
   You can click **Clear** to clear all the check boxes, and then select just the few cameras that are allowed.
9. Allow or deny access to the following functions:
   - **Right click menu**: right-click to change the resolution or to de-warp 360° camera images in the live view
   - **Snapshot**: take a snapshot of the video that is available in the live view
   - **Recordings**: record the video images in the live view
   - **Enable bounding boxes**: switch bounding boxes on or off in the live view.
10. Click **Apply**.
11. Click **Save**.

> ***Note***
>
> All other functions in the **Live Video** window are by default accessible to every user.

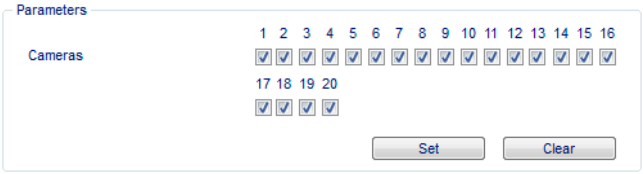
18.4.2 Recorded Video

Define whether or not the specific user can watch recordings via **Timeline/Postmotion** and back up recordings. Proceed as follows:

1. In the access rights panel, choose **Recorded Video > Timeline/Postmotion**.



2. Click **Deny** if you do not want the user to access the **Recorded Video** window. In this case, you can skip all following steps. If you allow the user to access the **Recorded Video** window, continue with the setup.
3. To define which cameras the user can access, click **Cameras**. By default all cameras are selected.



4. Clear the check boxes for the cameras that this user is not allowed to view, and click **Set**.
   You can click **Clear** to clear all the check boxes, and then select just the few cameras that are allowed.
5. To allow or deny backup, click **Backup**.
6. Click **Apply**.
7. Click **Save**.

> ***Note***
>
> If the user cannot watch recordings, the user also cannot backup any recordings.

18.4.3 System

Define whether or not the specific user has access to the system settings. Proceed as follows:

1. In the access rights panel, choose **System > System**.
2. Click **Deny** if you do not want the user to access the **System** window. In this case, you can skip all following steps. If you allow the user to access the **System** window, continue with the setup.
3. Define the system settings to which the user has access. The user rights are grouped according to the main menu groups in the system settings pages:

- Connections
  - Ethernet
  - Serial
  - Video Inputs
  - Monitor
  - Audio
  - I/O
  - PresidiumHLI
  - Video interconnection
  - E-Mail
  - Active connections
- Behaviour
  - Arm/Disarm Schedule
  - Alarm Profiles
  - Input/Output Behaviour
  - CMS Alarm Transmission
  - Analytics
    If you allow access to the **Analytics** settings, then also define for which cameras
  - PIR
  - Access control
  - Recording
  - E-Mail Addressbook
- General
  - Date/Time
  - Calendar
  - Users
- Maintenance
  - Log
  - Transfer
  - Harddisks
  - Hipi/Eth config
  - Configuration Management

4. Select or clear the desired check boxes.
5. Click **Apply**.
6. Click **Save**.

18.4.4 Status

Define whether or not the specific user has access to the **Status** page. Proceed as follows:

1. In the access rights panel, choose **Status > Status**.
2. Click **Deny** if you do not want the user to access the **Status** window. In this case, you can skip all following steps. If you allow the user to access the **Status** window, continue with the setup.
3. To allow or deny isolating alarm inputs, click **Isolate**, and then click **Allow** or **Deny**.

4. To allow or deny manually activating inputs, click **Activate outputs**, and then click **Allow** or **Deny**.
5. Click **Apply**.
6. Click **Save**.

18.4.5 General

Define whether or not the specific user has access to some general functions. Proceed as follows:

1. In the access rights panel, choose **General**.
2. Click **Set tech rights**, and then click **Allow** or **Deny** to define if the user is allowed to grant access for the Technician users. For more information, see *Granting the Technician* on page 140.
3. Click **Arm/disarm**, and then click **Allow** or **Deny** to define if the user can arm or disarm the video system (change the operational mode). See *Operational Mode with Manual Selection* on page 64.
4. Click **Audio talk**, and then click **Allow** or **Deny** to define if the user can use the microphone to talk to people on-site. See *Audio* on page 77.
5. Click **Apply**.
6. Click **Save**.

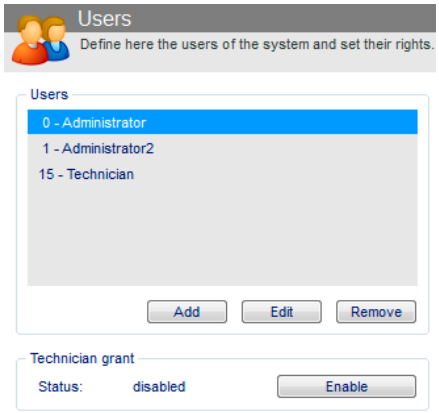
18.5 Modifying or Deleting an Existing User

Only Administrator users can modify or delete users. Normal users and Technicians can only modify their own user profile.

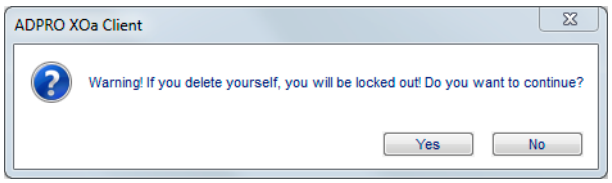
> ***Note***
>
> You cannot delete users 0 (Administrator) and 15 (Technician).

To modify or delete an existing user, proceed as follows:

1. Choose **System > General > Users**.



2. To modify a user, click the desired user, and then click **Edit**.
3. Change the required settings, and then click **Apply**.
4. Click **Save**.
5. To delete a user, click the desired user, and then click **Remove**.
   If you try to delete your own user profile, the following warning appears:



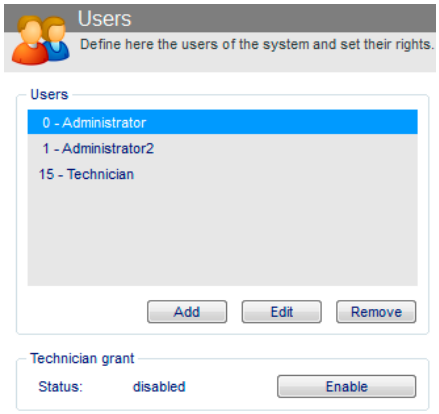
> ***Caution!***
>
> If you delete your own user profile, you will not be able to log on again. You will lock yourself out of the system.

6. Proceed as follows:
   - Click **No** if you want to keep your user profile.
   - Click **Yes** to delete your own user profile. The system restarts, and you cannot log on anymore with your user credentials.

18.6 Granting the Technician

To grant access to Technician users, proceed as follows:

1. Choose **System > General > Users**.



2. In the **Technician grant** pane, click **Enable**.
3. To deny access to the Technician users, click **Disable**.

> ***Caution!***
>
> The system automatically disables the technician grant when you reboot the server. Closing and opening the client does not affect the technician status.

19 Uploading and Downloading Files

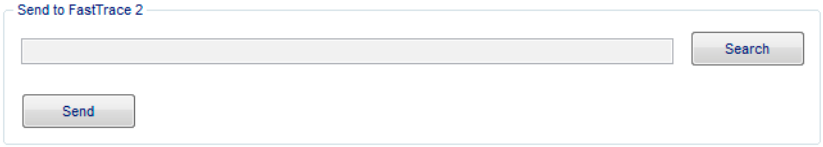
19.1 Uploading Files to the Server

It is possible to upload different types of files to the server. You can recognise the file type by the file extension:

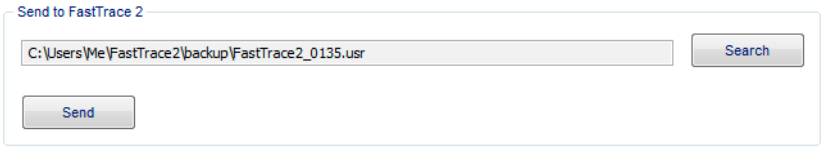
- .bin = software (Linux + application)
- .lic = license
- .usr = user data
- .prop = configuration
- .def = camera definitions

To upload a file to the server, proceed as follows:

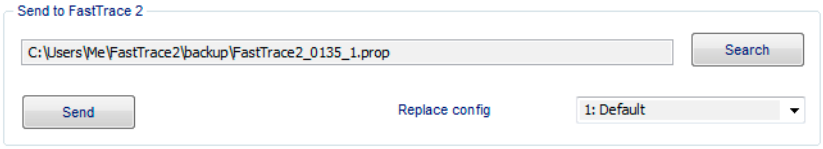
1. Choose **System > Maintenance > Transfer**.



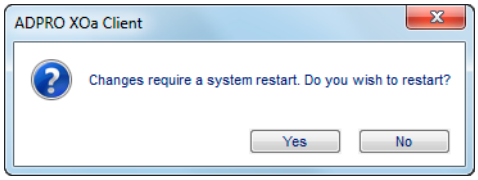
2. In the **Send to server** pane, click **Search**.
   Select the file that you want to upload and click **Open**.



3. If you are uploading a configuration file, select the configuration that you want to overwrite in the **Replace config** box.



4. Click **Send** to upload the file to the server.



5. Click **Yes** to restart the server and apply the new settings (e.g. license).

Note

You can download a license from a server on firmware version 2.5 (or lower version) and upload this license into a server on firmware version 2.6. Although the license formats have changed in the new firmware version 2.6, the “older” license will be automatically converted.

However, it is not possible to load a license file from a server on firmware version 2.6 into a server on firmware 2.5 (or lower).

Note

A full upgrade of the firmware and software may cause your data to get lost (e.g. license, user data, configuration…). Make sure you have downloaded these files from your video system before you start upgrading.

(See *Downloading Files from the* Server on page 142.)

If, by accident, you do lose your configuration, you will need to redo all settings in the video system.

If you also lose your system license, you will need to contact your supplier (Xtralis Support) to retrieve a new license. If a new license needs to be retrieved from Xtralis Support, you will need to provide the serial numbers of your video cards. Click **About** in the top menu to see the system information, which contains the serial numbers. Click the **Clipboard** button to copy the information, and then paste it into an email to Xtralis Support.

Note

Xchange is the new platform that allows you to easily activate and deploy additional applications, and upgrade firmware on your RMG devices. For more information, see the *Xchange Tool User Manual*.

19.2 Downloading Files from the Server

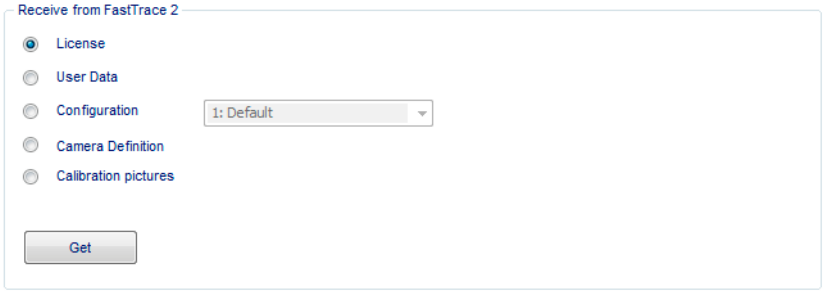
Before installing new software, or before making major changes to the configuration, it is recommended that you download the following files to your local hard disk:

- Licenses
- User data
- Configurations
- Camera definitions
- Calibration pictures.

If you lose any of the above data or settings, you can upload the downloaded files again to restore settings.

To download files from the server, proceed as follows:

1. Choose **System > Maintenance > Transfer**. For downloading, you use the **Receive from server** pane.



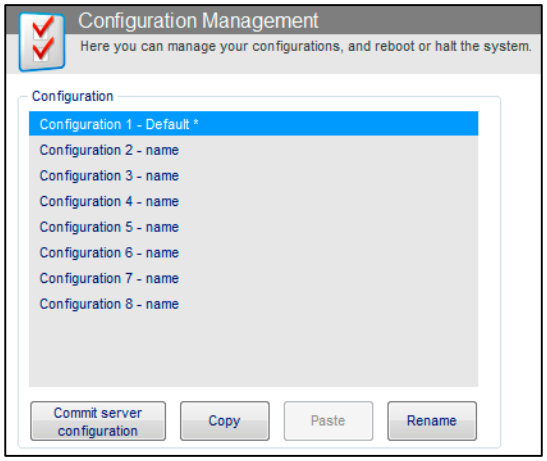
2. To download the licenses, click **License**, and then click **Get**.
3. Select the destination folder and click **OK**.
4. To download user data, click **User Data**, and then click **Get**.
5. Select the destination folder and click **OK**.
6. To download a configuration, click **Configuration**.
7. Select the desired configuration from the list, and then click **Get**.
8. Select the destination folder and click **OK**.
9. Repeat for each configuration.
10. To download the camera definitions, click **Camera Definition**, and then click **Get**.
11. Select the destination folder and click **OK**.

20 Configuration Management

20.1 Storing a Configuration

The video system can store up to 8 different configurations. Only 1 configuration can be active. The server stores any changes you make in the active configuration (if you save the changes). Any unsaved changes are lost when you close the client software.

To open the **Configuration Management** window, choose **System > Maintenance > Configuration Management**. The list of configurations appears. An asterisk (*) marks the active configuration.



To store the current settings in the **active** configuration (in the example above: **Configuration 1 – Default ***), click **Commit server configuration**.

> ***Caution!***
>
> When you click **Commit server configuration**, the video system stores the current settings in the **active** configuration (= the configuration marked by an asterisk (*). It **does not store** the settings in the **selected** configuration (= the configuration that is highlighted in the list).
>
> If you want to store the current settings in a **different** configuration, you must first store the settings in the active configuration, and then **copy** the active configuration into the other configuration.

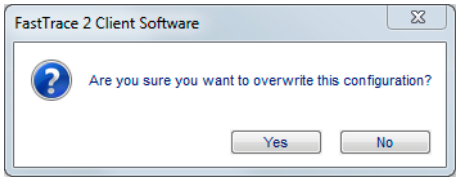
Xtralis recommends using a meaningful and relevant name for the configurations. To change the name of a configuration, select the configuration in the list and then click **Rename**. Type the name in the **Name** box and click **OK**.

20.2 Copying Configurations

If you want to use a new configuration, you do not have to set up the configuration from scratch. You can copy the settings from any existing configuration to the new one. Afterwards, you can make the necessary changes to the new configuration.

To copy the settings of one configuration to another, proceed as follows:

1. In the list of configurations, click the configuration that you want to copy from.
2. Click **Copy**.
3. In the list of configurations, click the configuration that you want to copy to.
4. Click **Paste**. The following message appears:



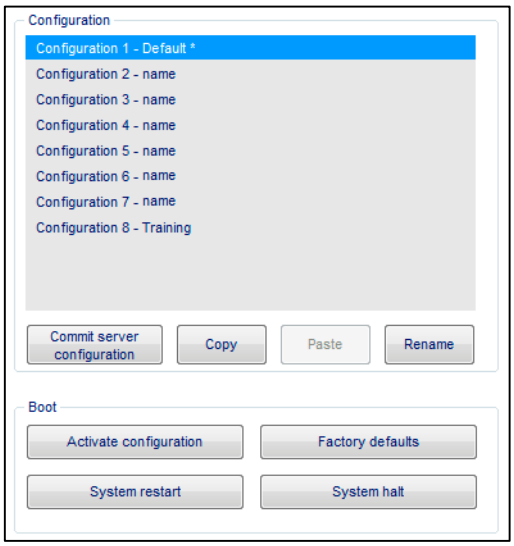
5. Click **Yes** to confirm.

20.3 Activating a Configuration

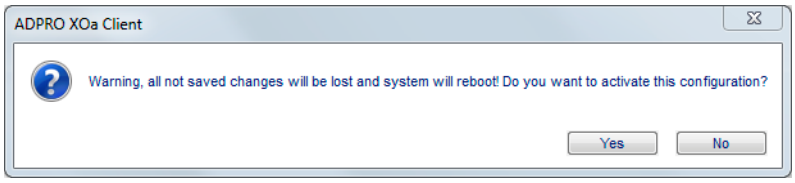
> ***Caution!***
>
> Be very careful when activating a different configuration. If settings are missing or incorrect in that configuration, your RMG device may become unusable or unreachable (for example, if the IP address changes). Xtralis recommends to start from a configuration that works well, copy that into a new configuration, and then activate the new configuration so you can make the necessary changes.

To activate a configuration, proceed as follows:

1. Choose **System > Maintenance > Configuration Management**.



2. Click the desired configuration in the list, and then click **Activate configuration** (or double-click the configuration). The following screen appears:


ADPRO XOa Client
Warning, all not saved changes will be lost and system will reboot! Do you want to activate this configuration?
Yes
No

3. Click **Yes** to confirm.
4. Wait for the server to reboot, and then open the client again. The selected configuration now has an asterisk in the list of configurations.

21 Factory Defaults

It is possible to reset the server to the factory defaults. This means that all modifications made to the configuration will be lost. Your server will also lose all camera settings (and provide 4 analogue cameras).

Open **System > Maintenance > Configuration Management**. When you click the **Factory defaults** button in the **Boot** pane, all modified configurations will be deleted. Your video system will also be given the default IP address 10.0.0.10. The unit will automatically reboot.

22 Starting and Stopping

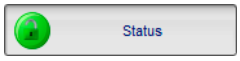
You can restart the server by clicking **System restart**.

If you want to stop the server, click **System halt**. If you do not switch off power, the server will automatically reboot after 20 seconds. It is recommended to halt the system before switching off power.

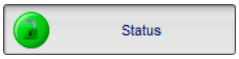
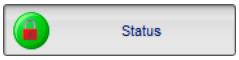
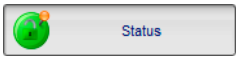
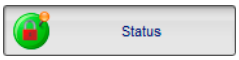
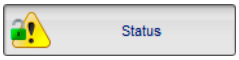
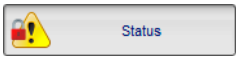
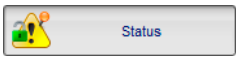
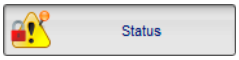
23 Status

23.1 Status Indicators

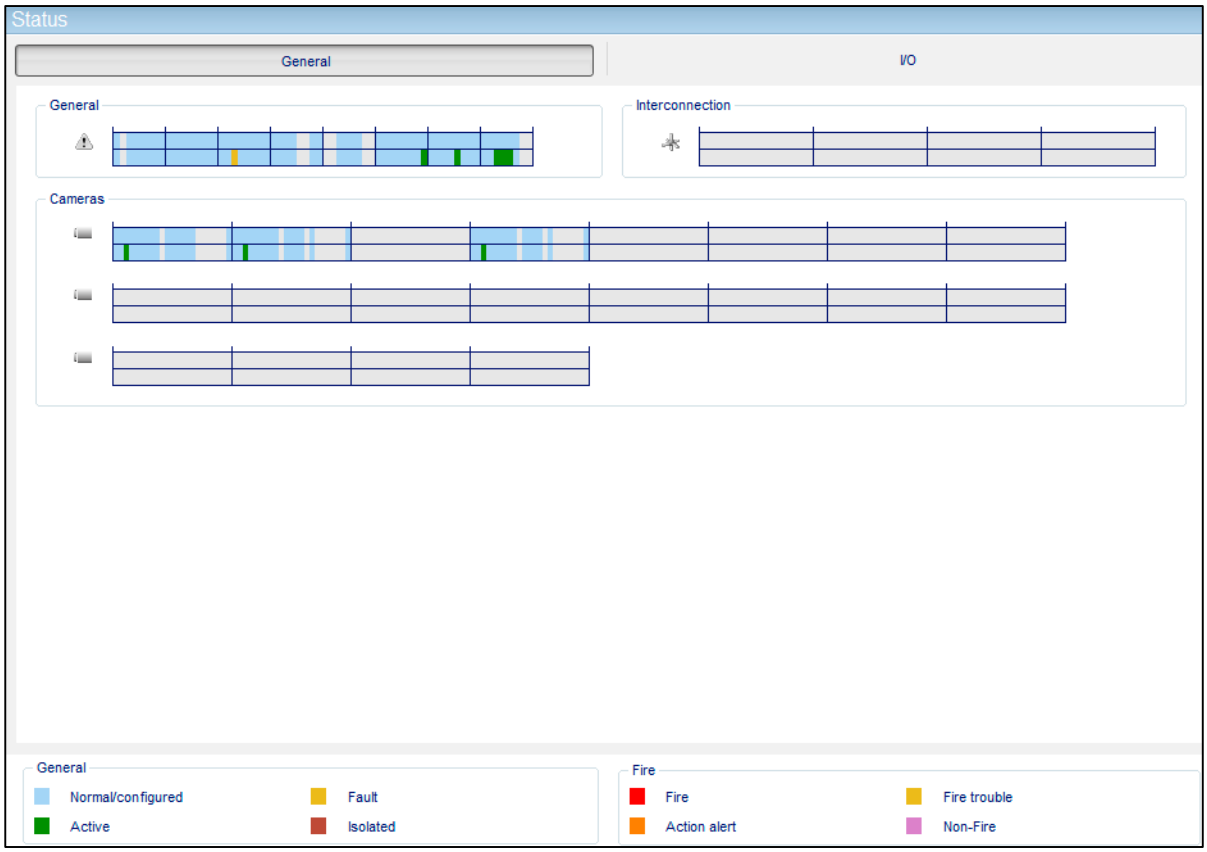
Click **Status** in the top menu to see the status of all cameras, the video system, and all inputs and outputs.



The button itself looks different depending on the system status, providing basic information:

Button	Description
	Normal disarmed status. • The green circle indicates that there are no active faults. • The green padlock indicates that the system is disarmed.
	Normal armed status. • The green circle indicates that there are no active faults. • The red padlock indicates that the system is armed.
	Normal disarmed status with isolated alarm/input. • The pin indicates that there is at least one isolated fault/input. • The green circle indicates that there are no active faults that are not isolated. • The green padlock indicates that the system is disarmed.
	Normal armed status with at least one isolated fault/input.
	Fault in disarmed status. • The yellow warning sign indicates that there is at least one active fault. • The green padlock indicates that the system is disarmed.
	Fault in armed status.
	Fault in disarmed status with isolated fault/input.
	Fault in armed status with isolated fault/input.

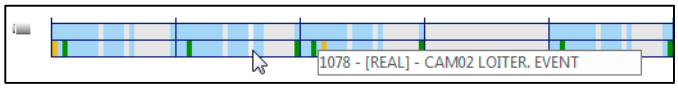
Click the **Status** button to see an overview with different status bars.



The **General** tab displays the information about the general RMG system, the interconnection, and the cameras.

The **I/O** tab displays the information about on-the-box inputs and outputs (Main and Extension I/O), IP camera inputs and outputs, workbit inputs and outputs, PIR inputs, and the analytic detail status inputs.

Place the mouse pointer on an indicator (status bar) to see a detailed description.



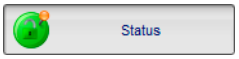
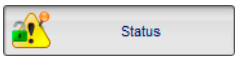
The bar colour indicates the status. The **General** pane (at the bottom of the screen) displays an overview of the colours and a short explanation of their meaning:

Colour	Description
	A light blue bar indicates that the item is in the normal state, or that it is configured. For example, the bar CAMxx PERIMETER for a camera is blue if IntrusionTrace is active on the camera, but no intrusion is detected at the moment.
	A green bar indicates that the item is active and working without faults. For example, the bar 0510 – [SYST] – GENERAL RECORDING is green when the video system is recording.
	A yellow bar indicates that there is a fault, and that you must take action. For example, the bar CAMxx PERIMETER for a camera is yellow if IntrusionTrace is detecting an intrusion at the moment.
	A brown bar indicates that the input/fault is isolated.

23.2 Isolating an Alarm Input

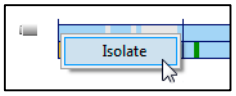
Isolating an alarm input means the alarm is no longer received. The isolated input is marked in brown in the **Status** window.

When you isolate an input, the video system activates input I0511, and transmits the system message 0511 – [SYST] – GENERAL ISOLATION every 24 hours until you activate all isolated inputs again. The **Status** button in the top menu changes shape: an orange coloured pin indicates that there are isolated inputs.

	One or more inputs are isolated; there are no other (not isolated) faults.
	One or more inputs are isolated; there are other (not isolated) faults that you need to check.

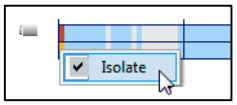
To isolate an alarm input, proceed as follows:

1. Click **Status**, and then click the tab that displays the input (**General** or **I/O**).
2. Right-click the desired input, and click **Isolate**.



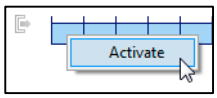
The status bar colours brown.

3. To re-activate an isolated input, right-click the desired input again, and click **Isolate**.



23.3 Activating an Output Manually

To manually activate an output, right-click the desired output and click **Activate**.



Note

You cannot activate an output that is already active (= green colour). It is also not possible to manually deactivate an active output.

23.4 General Status of the Video System

You can receive one of these messages when checking the status of your cameras, video system, and inputs and outputs.

Cam x past analytics	Error during post motion analysis – contact your dealer.
Cam x sab analytics	Error in camera tampering analysis – contact your dealer.
Cam x recording	Camera images are currently being recorded to hard disk.
Cam x synch fault	No video signal on camera – check camera power supply or coax cable.
Cam x Contrast fault	Camera lens covered or lighting suddenly switched off.
Cam x Sabotage fault	Camera displaced or lens fault or zoom/focus settings changed.

Cam x event	User programmable camera event – has to be activated by a logical function.
Cam x live view	The Live Video view is displaying live images of this camera.
Config uncommitted	Current configuration is not yet saved. Restarting the system may cause loss of latest modifications.
Encoder card error	Video capturing card or HIPI card out of order. Could indicate a hardware fault. All cameras on associated card will not work.
License error	Wrong license has been loaded or no license at all.
HD error	Hard disk fault. Requires hard disk replacement.
HD full	Hard disk full. Too many recordings are stored on hard disk.
HD corrupt	Indicates corrupt data – contact your dealer.
Db error	Indicates corrupt or unreadable data files – contact your dealer.
Entry error	Not disarmed in time on entry.
Exit error	Area not abandoned in time on exit (after arming the system).
Modem init failed	Modem not ready/not connected.
Primary line fault	Primary connection not ready.
Primary lifecheck	Life check sent over primary connection.
Backup line fault	Backup connection not ready.
Backup lifecheck	Life check sent over backup connection.
AL tx queue overflow	Alarm buffer overflow – too many alarms or unable to transmit alarms to CMS.
Recorder overflow	Too many recordings on the same day – system switches to continuous recording.
Event queue overflow	Too many events on the same moment. Restart the client to reset the error.
Sensor activity	Critical inputs are active – system should not be armed.
General power	Indicator – power supply OK.
General fault	Indicator – fault condition.
General recording	Indicator – System is recording.
General isolation	Indicator – One or more inputs have been isolated by user.
General mode 1–4	Indicator – System is currently in mode 1–4.
SMART HDD error SMART HDD alert SMART HDD temperature	Analytical information received from the hard disk (SMART).

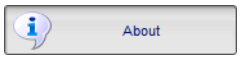
24 System Information

24.1 Checking the Firmware and Software Version

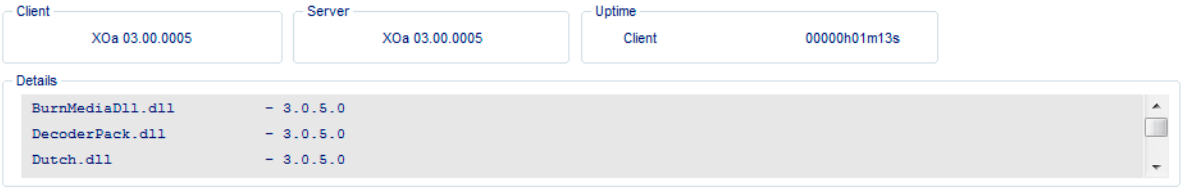
At regular times new firmware and software updates are released. You can download these new releases using the Xchange Tool. For more information, see the *Xchange Tool User Manual*.

To check the version of your system (server and client), you can use the client software.

Click **About** in the top menu.



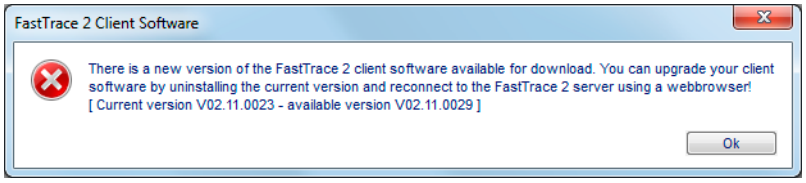
You will get the information about the XOa client version and the server version:



You can also check the firmware versions of the different dll files that are used by the server.

The *Uptime* section shows how long you have been connected to the server with this client software.

It is always recommended to have both client and server on the same version, but in principle different versions can be used. When your client software is older than the firmware version on the server, the following warning message appears when you start the client software:


FastTrace 2 Client Software
There is a new version of the FastTrace 2 client software available for download. You can upgrade your client software by uninstalling the current version and reconnect to the FastTrace 2 server using a webbrowser!
[Current version V02.11.0023 - available version V02.11.0029]
Ok

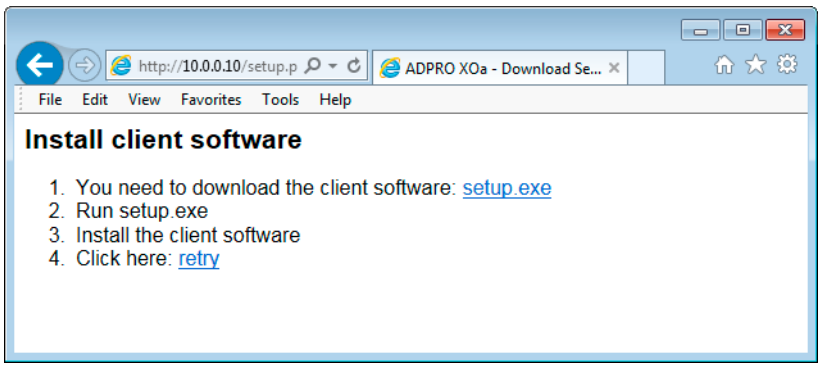
Click **OK** to close the message box. The client software opens, but the following warning appears:

Note that the **System** menu is unavailable until you update the client software.

To update the client software, proceed as follows:

1. Close the XOa client software.
2. Open your web browser.
3. In the address box, type the server's IP address followed by /setup.php. For example: http://10.0.0.10/setup.php

   The following window appears:

   
   http://10.0.0.10/setup.p
ADPRO XOa - Download Se...
File Edit View Favorites Tools Help
Install client software
1. You need to download the client software: setup.exe
2. Run setup.exe
3. Install the client software
4. Click here: retry

4. Click **setup.exe** to download the setup file.

5. Click **Run**, and then follow the instructions of the installation Wizard.
Alternatively, you can download the installation file, and launch it from the download folder.

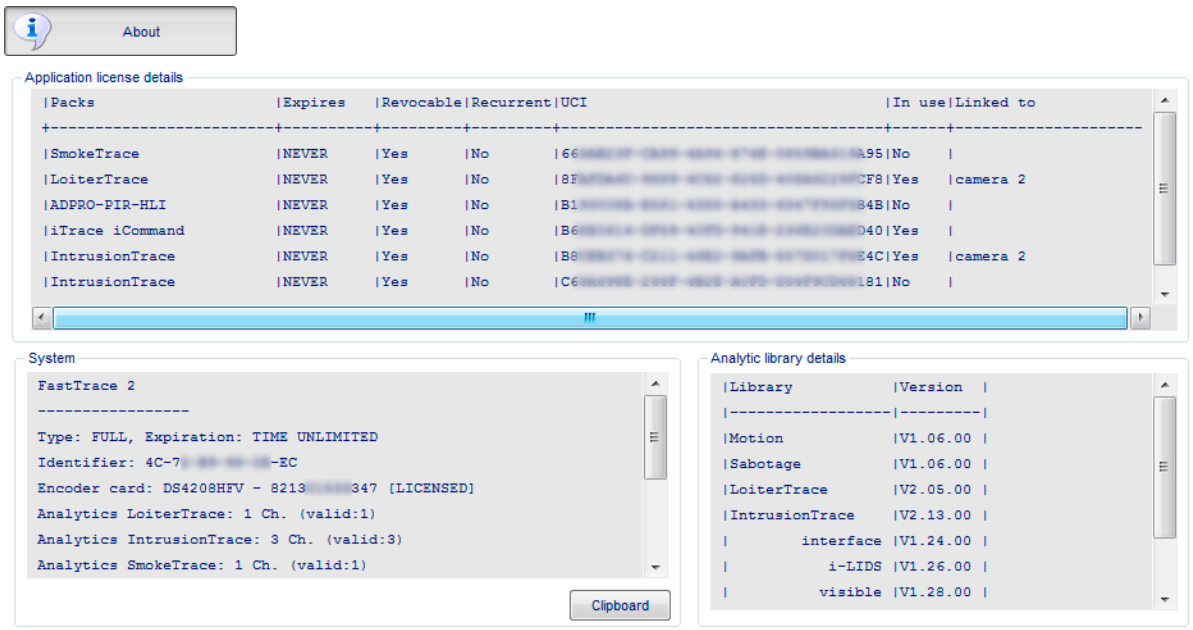
> ***Note***
>
> After a software update, the RMG starts optimising the recording disks. During this optimisation process, the video system does not record, and the system may display an error message to indicate this. When the optimisation process is finished, recording restarts automatically. The time needed for optimising the disks depends on the number of disks, the amount of video data on the disks, etc.

24.2 Licenses

You can load different types of licenses in the video system:

- System license
For more information, see *System License* on page 153.
- Encoder license = a license for the analogue video cards in the video system
- Application license = a license for using an extra application. For more information, see *Application Licenses* on page 154.

To see which licenses are available on your video system, click **About** in the top menu.



The different panels display the following information:

- **Application license details**: a list of all installed application licenses, their expiry date, if they are revocable, if they are recurrent, ID, if the licenses are in use or not, and the camera to which they are assigned.
- **System**: system information such as the system license, identifier (MAC address), encoder card licenses, analytics channels, motherboard type…
You can click **Clipboard** to copy the system information. You can then, for example, paste the system information into an email to Xtralis technical support staff.
- **Analytic library details**: version numbers of the libraries for analytics.

If you do not have access to the XOa client software, you can use the **ta,license** command in a Telnet session to display the license information.

24.2.1 System License

From version 2.00, all ADPRO video systems require a system license.

> ***Note***
>
> Applications such as IntrusionTrace, LoiterTrace…, and the video encoder cards require a separate license. They are not included in the system license.

There are 3 types of system licenses available:

- FULL: all features of the video system are available.
- ENTRY(*): all features are available, with these restrictions:
  - You can use only 4 analogue cameras (no IP camera support).
  - You can use only 1 hard disk.
  - You can only use 1 MIO card (and no EIO cards).

- TRANSMITTER (TX) only: all features are available, but continuous recording is not allowed and recording on event is fixed to 5 seconds pre-recording, 10 seconds event recording, and 0 seconds post-recording. Furthermore, event recording stops when the limit of 16,000 events has been reached.

(*) The ENTRY system license is not available for the FastTrace 2X or FastTrace 2E configuration.

An RMG video system running without system license will behave as a video system with a **FULL license for 5 days**. However, the system informs the user of the license error via the event message 0013 – [SYST] – SYSTEM LICENSE ERROR, and via a popup window at each connection with the XOa client.

After that period of 5 days, the video system enters a **locked-down state**, and refuses all connections for live streams and recordings. All active configured recordings continue on the video system. During this locked-down state, the XOa client shows only the **About** window (so that you can retrieve the necessary information to order a new license) and the **Transfer** window (so that you can upload a license to the RMG video system). For more information on uploading licenses, see *Uploading Files to the Server* on page 141.

Note

The system license is locked on the RMG motherboard and is therefore system specific: the license must include the correct MAC address.

When you upload the system license and your unit already has other licenses (e.g. an encoder license, a LoiterTrace license…), your video system merges all these licenses together in one license file. For backup and archiving, you only need to download one file.

24.2.2 Application Licenses

The ADPRO FastTrace 2/2X/2E platforms – from version 2.6 onwards – provide the ability to unlock extra functionality that resides in its system firmware. To unlock functionality, you need to buy an **application license** via your regular Xtralis sales channel.

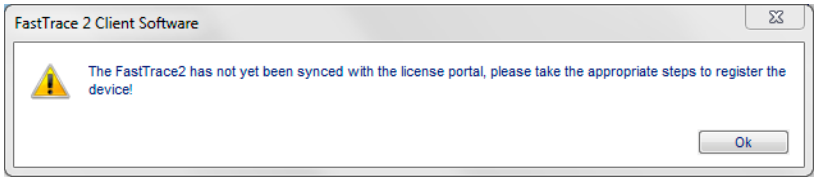
You can add the following applications to the RMG functionality:

- ClientTrace: video analytics application for business intelligence, detecting the presence of potential customers
  For more information, see the ClientTrace documentation.
- IntrusionTrace: video analytics application for video perimeter detection
  IntrusionTrace PLUS: IntrusionTrace including PIR-HLI
  For more information, see the IntrusionTrace (PLUS) documentation.
- iTrace iCommand: additional verification and response capabilities for iTrace
  For more information, see the iTrace documentation. The iTrace iCommand features are included in the XOa 3 software, free of charge.
- LoiterTrace: video analytics application for indoor loitering detection
  For more information, see the LoiterTrace documentation.
- PIR-HLI: interface application for alarm reception, configuration, and walk testing using the PRO detectors databus
- SmokeTrace: video analytics application for smoke verification
  For more information, see the SmokeTrace documentation.

When you buy an application license, you receive a **credit token** with a code. You redeem the credit token in the Xtralis Xchange tool, and then you can install the application license on the desired RMG unit. For more information on handling application licenses for RMG, see the *Xchange Tool User Manual*.

There are **perpetual licenses**, and **timed licenses**. A perpetual license never expires, whereas a timed license expires, for example, one year after the license has been deployed on a RMG unit for the first time. When the license expires, the application stops working. It is the responsibility of the user/installer of the system to replace the license in time. The RMG unit transmits expiry notifications when the license expires. From then, you have a grace period of 30 days during which you can renew the license. To make sure that you receive the expiry notifications, see *Tech Tip 5 – Managing Timed Licences*.

When you upgrade to software version 2.6, the system automatically converts your existing analytics licenses to the new license formats. The following warning appears:


FastTrace 2 Client Software
The FastTrace2 has not yet been synced with the license portal, please take the appropriate steps to register the device!
Ok

You need to synchronize your RMG unit with the licenses portal. For more information, see the *Xchange Tool User Manual*.

24.3 Viewing Active Connections

The **Active connections** window displays the active client protocol connections and the active RTSP connection. You cannot modify any settings in this screen; it is for information only.

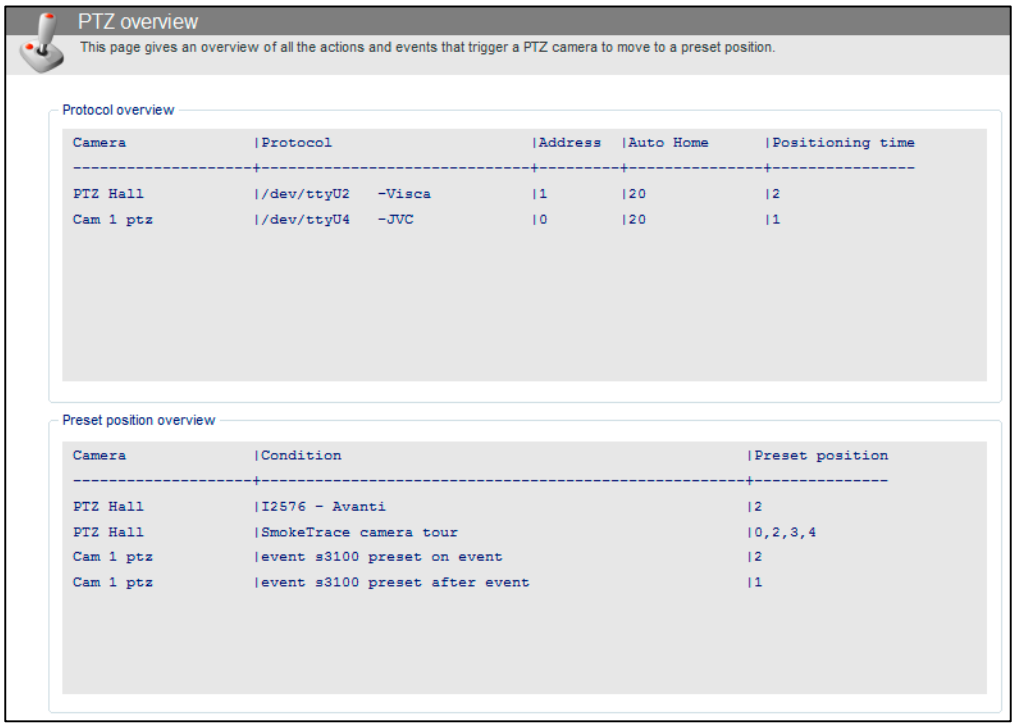
To see the active connections, choose **System > Connections > Active connections**.

Active connections
Here you can view the active video and control connections
Active video connections
|IP address |Port |User |Cam|Connection start time|Stream Type|Fps|Resolution
|10.0.0.21 |11576 |0 |1 |14/09/12 - 14:05:07 |live |n/a|n/a
Active control connections
|IP address |Port |User |Connection start time|CMS
|10.0.0.21 |14189 |0 |14/09/12 - 13:58:40 |*

The upper section displays the active video connections (= active RTSP connection). The lower section displays the active control connections (= active client protocol connections).

24.4 PTZ Overview

The PTZ overview screen displays an overview of PTZ camera configurations, and of the configured PTZ presets that the RMG can trigger. It includes the presets on and after event recording conditions, on I/O triggers, and for SmokeTrace. You cannot modify any settings in this screen; it is for information only.


PTZ overview
This page gives an overview of all the actions and events that trigger a PTZ camera to move to a preset position.
Protocol overview
Camera |Protocol |Address |Auto Home |Positioning time
PTZ Hall |/dev/ttyU2 -Visca |1 |20 |2
Cam 1 ptz |/dev/ttyU4 -JVC |0 |20 |1
Preset position overview
Camera |Condition |Preset position
PTZ Hall |I2576 - Avanti |2
PTZ Hall |SmokeTrace camera tour |0,2,3,4
Cam 1 ptz |event s3100 preset on event |2
Cam 1 ptz |event s3100 preset after event |1

The sample screen above shows the following information:

Item	Description
Protocol overview	
Camera	The PTZ camera name.
Protocol	The port and PTZ protocol.
Address	The camera address for PTZ control.
Auto Home	The time (in seconds) after which the camera moves back to its home position.
Positioning time	The delay (in seconds) for the corresponding alarm message.
Preset position overview	
Camera	The PTZ camera name.
Condition	The trigger that instructs the camera to move to a preset position. The example screen shows: • The number and name of an input (I2576) that triggers camera ‘PTZ Hall’ to move to preset position 2. • A SmokeTrace trigger for camera ‘PTZ Hall’ to move to preset positions 0, 2, 3, and 4. • Event triggers: ‘event S3100’ triggers camera ‘Cam 1 ptz’ to move to preset position 2 on the event, and back to preset position 1 after the event.
Preset position	The number of the position that the camera moves to.

24.5 Logs

24.5.1 About Logs

Local legal requirements (variable and depending on state and region, please check with your local authorities) may stipulate that a video system has to keep a logbook (e.g. the Law Sarkozy in France). The logbook, or log for short, registers all user interventions and events.

The server offers different log types with different information, to make it easier to keep an overview and find the data you need.

Note

A log is limited to 100 000 events per type (log, event, or command; see below) and has a time period limit of 6 months. RMG automatically deletes any logged data older than 6 months. If you need to keep logged data longer than that, you can save the log on a local hard drive or USB stick.

The following log types are available:

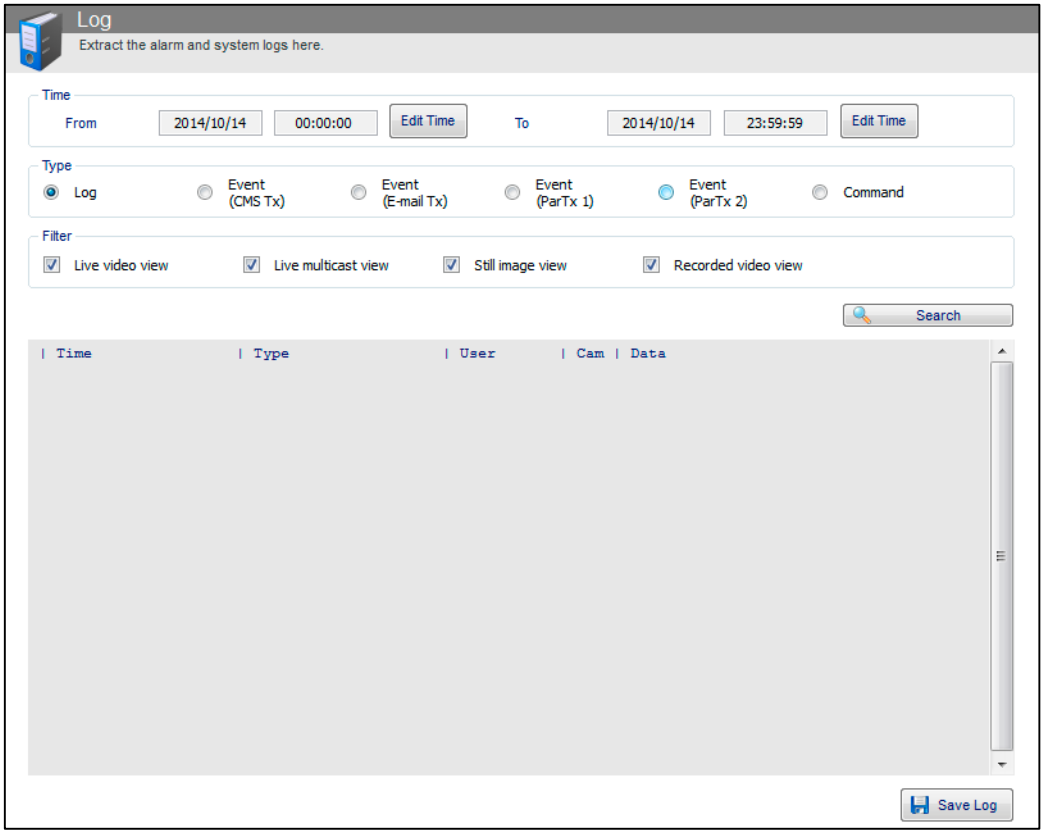
Log	Log of users and what they viewed. You can filter the log to display one or more of the following view types: • **Live video view**: lists the users that started a live video stream. • **Live multicast view**: lists the users that started a live multicast video stream. • **Still image view**: lists the users that viewed still images = starting/stopping playback of recorded video. • **Recorded video view**: lists the users that watched or downloaded recorded video.
Event (CMS Tx)	Log of events that are configured for transmission to the CMS. You can filter the log to display one or more of the following event types: • **Faults**: alarms and errors, such as tamper alarms, locked recordings, etc. • **Fire**: fire events. • **Other**: other events that are not faults or fire events, such as system messages, motion detection, live viewing, inputs and outputs, etc.
Event (E-mail Tx)	Log of events that are configured for transmission to email. You can filter the log using the same event types as described for transmission to the CMS.
Event (ParTx 1)	Log of events that are configured for transmission to parallel destination 1. You can filter the log using the same event types as described for transmission to the CMS.
Event (ParTx 2)	Log of events that are configured for transmission to parallel destination 2. You can filter the log using the same event types as described for transmission to the CMS.
Command	Log of users and the commands that they executed, such as connecting to servers, saving configurations, etc.

Note

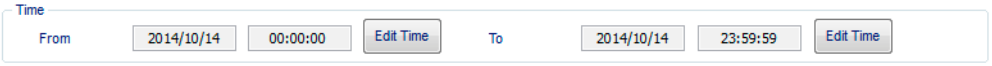
The logs contain events that actually occurred, and that are configured for the selected transmission. However, this does not imply that the destination has actually received the event message. For example, if you set up LICENSE EXPIRED for email transmission, the event appears in the log when a license expires. However, if you did not set up a mailing list for it, then the message LICENSE EXPIRED does not reach any email destination.

To display a log, proceed as follows:

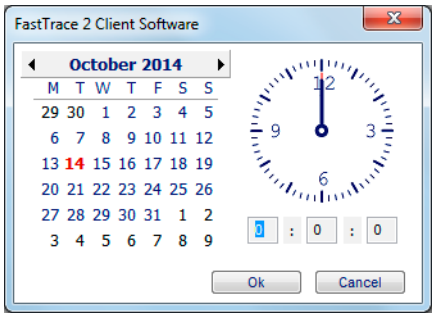
1. Choose **System > Maintenance > Log**.



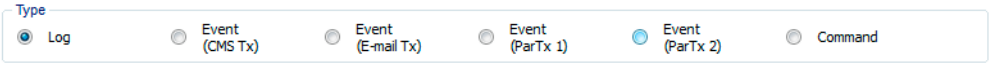
2. Under **Time**, set the desired time frame.



You can type the date and time indications in the **From** and **To** boxes, or you can click **Edit Time** to select a date and set a time:

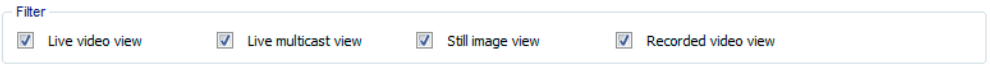


3. Under **Type**, select the type of log data that you want to display.

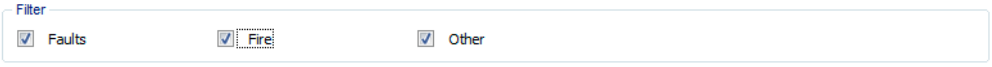


4. Under **Filter**, select the log or event types that you want to include in the log.

Log filters:



Event filters:



5. Click **Search** and wait for FastTrace to display the requested data.
Retrieving the data may take several minutes. In this case, you can click **Stop** to stop data retrieval. You can then shorten the time frame or adjust the filters, and try again.

For examples of log data, see the sections further below.

24.5.2 Saving a Log

You can save a log file in text format (.txt) to your local hard disk. You can open the log files in any text editor, such as Notepad.

The file name indicates the type of log (log, event, command) and the timeframe. For example:
Command 2014-11-06 00-00-00 -- 2014-11-06 23-59-59.txt
This file contains the command log of November 6, 2014.

The first line of the log file contains the RMG unit ID, the site name, the IP address, the type of log, and the timeframe:

```
0001 - FT2 MainBuilding (10.0.0.1): Command 2014-01-01 00-00-00 -- 2014-11-06 23-59-59
--------------------------------------------------------------------------------
| Time                | Id  | Group          | Command             | Data
| 2014/11/06 09:21:57 | C26 | transfer       | download            | camera definitions
| 2014/11/06 09:21:57 | C26 | transfer       | download            | user data
| 2014/11/06 09:21:56 | C26 | login          | user                | (00) => authorized
| 2014/11/06 09:21:56 | C26 | connection     | open                | (10.0.0.2         )
| 2014/11/06 09:21:49 | C25 | connection     | closed              | (10.0.0.2         )
...
```

To save a log, proceed as follows:

1. Choose **System > Maintenance > Log**.
2. Generate the desired log data.
3. Click **Save Log**.
4. Browse to the desired folder and click **Save**.

24.5.3 Example of a Log Record

```
| Time                | Type                | User       | Cam | Data
| 2014/10/14 16:02:46 | Live video view     | 02         | 01  |
| 2014/10/14 16:02:46 | Live video view     | 02         | 05  |
| 2014/10/14 16:02:45 | Live video view     | 02         | 03  |
| 2014/10/14 16:02:45 | Live video view     | 02         | 02  |
| 2014/10/14 16:02:36 | Still image view    | 00         | 01  | 2014/10/14 16:02:33
| 2014/10/14 16:02:07 | Live video view     | 00         | 01  |
```

Time	Date and time when the event occurred
Type	View type (live video, recorded video…)
User	Number of the user that viewed the video
Cam	Number of the camera
Data	Additional information, for example the date/time of the still image.

24.5.4 Example of an Event Record

```
| Time                | Input/Output Behaviour                  | E | T | Quad ID              | Camera
| 2014/10/14 17:10:36 | I1162 - [REAL] - CAM05 MOTION1          | - | Q |                      |
| 2014/10/14 17:10:34 | I1182 - [REAL] - CAM05 CLIENTTRACE      | - | Q |                      |
| 2014/10/14 17:10:33 | I1162 - [REAL] - CAM05 MOTION1          | + | Q | 12400997607869506994 | 0000000
| 2014/10/14 17:10:33 | I1162 - [REAL] - CAM05 MOTION1          | - | Q |                      |
| 2014/10/14 17:10:30 | I0214 - [SYST] - RECORDING MATCH        | - | S |                      |
| 2014/10/14 17:10:30 | I0214 - [SYST] - RECORDING MATCH        | + | S |                      |
```

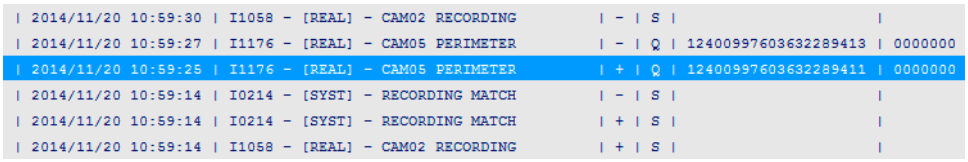
Time	Date and time when the event occurred
Input/Output Behaviour	Identification of the event: input/output number and name

E	Type of event: • +: start of the event • –: end of the event • R: repeated event
T	What the event triggers (corresponds with the **Camera view style** as defined for the input/output): • L: Live video • Q: Quad alarm • D: Duress (live + quad) • S: System event, does not trigger a camera view
Quad id	Identification number of the quad images that the event generated.
Camera mask	The camera mask indicates the cameras associated with the input/output, as defined in the input/output behaviour. For camera 1, the first digit counting from the right = 1. For camera 5, the 5th digit counting from the right = 1. If both camera 1 and 5 are associated with the input, both the first and the 5th digit = 1 (always counting from the right).
ATX	Alarm Transmission status: • blank = no transmission required • OK = transmission successful • NOK = transmission not successful
Alarm Time	Date and time of the alarm
Alarm Dest.	Alarm destination = the IP address of the destination where the alarm is sent to.
Data	Extra information, for example the IP address of the PC that establishes a remote connection.

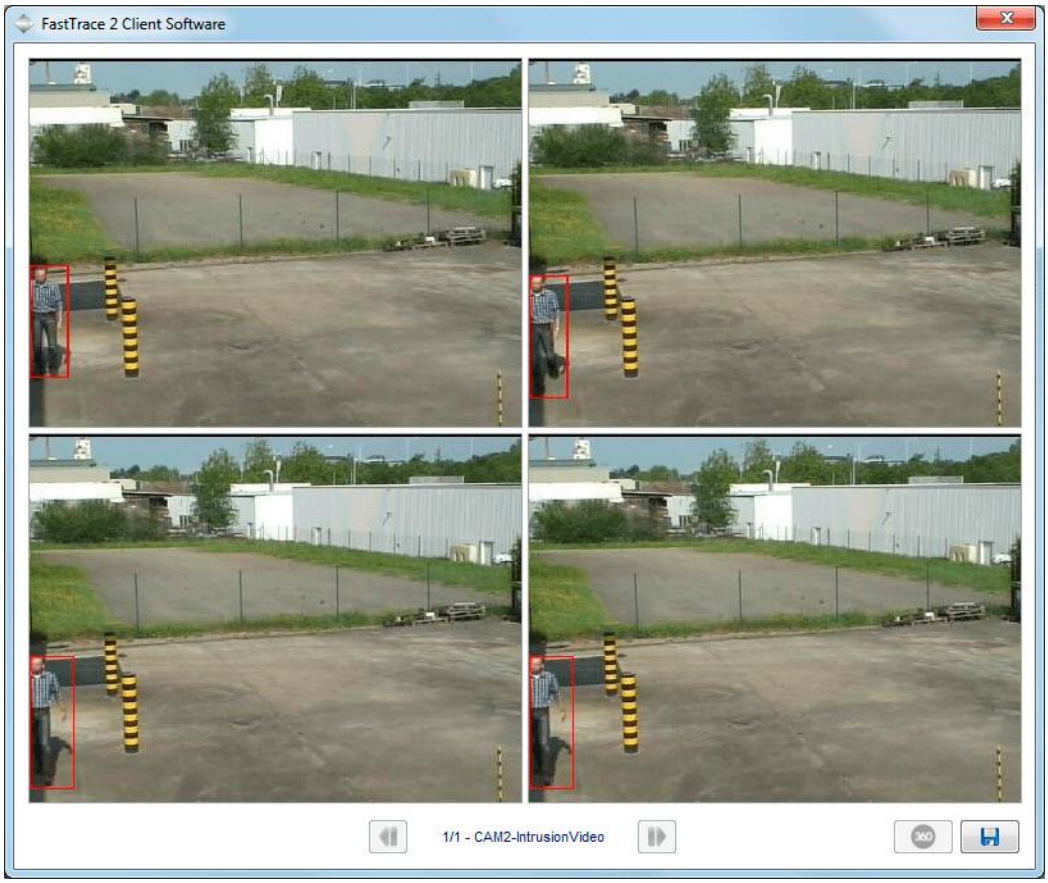
From the event log, you can display and save quad images that an event generated. This only works for **transmitted** quad images (ATX = OK).

To display quad images from the event log, proceed as follows:

1. In the event log, click the desired event line that has quad images:



2. Click **Show quads**. The quad images appear.



- If more than one camera is associated with the event, use the and buttons to browse through the different cameras.
- To save the currently displayed quad images, click . Browse to the desired storage folder and click **OK**. Repeat for images of different cameras.

3. Close the quad images screen to return to the event log.

24.5.5 Example of a Command Record

Time	Id	Group	Command	Data
2014/10/14 16:02:44	C08	transfer	download	camera definitions
2014/10/14 16:02:44	C08	transfer	download	user data
2014/10/14 16:02:43	C08	login	user	(00) => authorized
2014/10/14 16:02:43	C08	connection	open	(10.0.0.2)
2014/10/14 16:02:41	C07	connection	closed	(10.0.0.2)
2014/10/14 16:02:05	C07	transfer	download	camera definitions

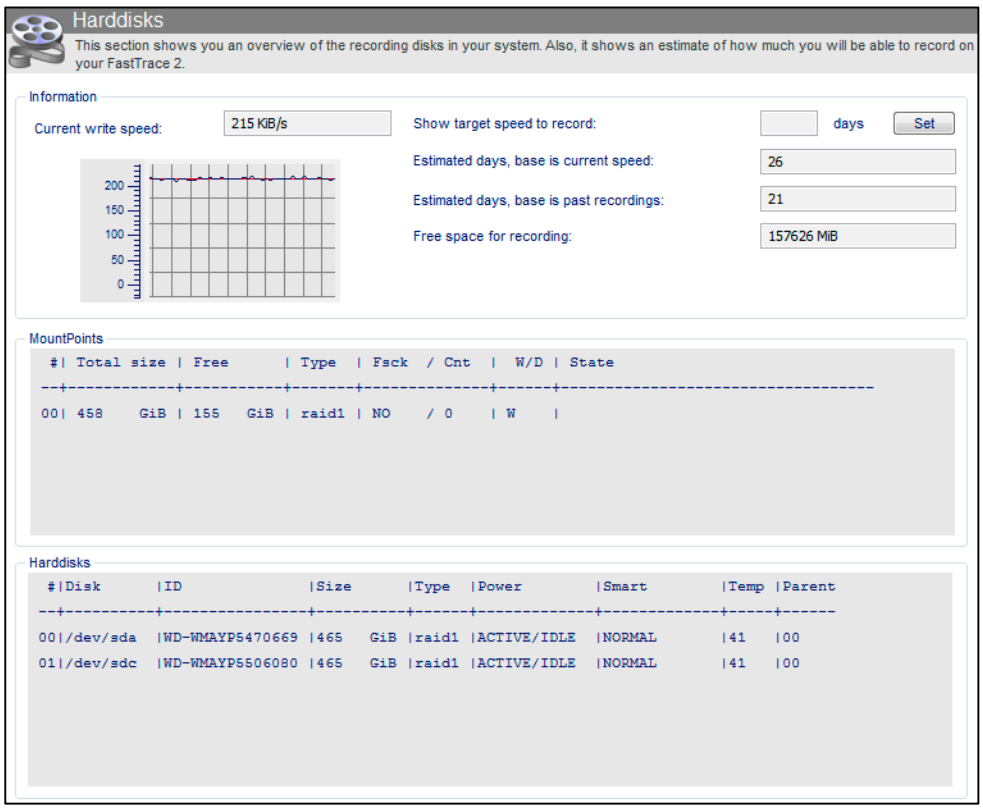
Time	Date and time when the command is executed
Id	Event identification*: • C = client session • T = Telnet session
Group	Specific command group
Command	Executed command
Data	Additional information (e.g. IP address)

* All commands within the same session have the same ID.

24.6 Hard Disks

Recordings are stored on the available hard disks in the server. The **Harddisks** window displays information about available storage space.

Open **System > Maintenance > Harddisks**.


Harddisks
This section shows you an overview of the recording disks in your system. Also, it shows an estimate of how much you will be able to record on your FastTrace 2.
Information
Current write speed:
215 KiB/s
Show target speed to record:
days
Set
Estimated days, base is current speed:
26
Estimated days, base is past recordings:
21
Free space for recording:
157626 MiB
200
150
100
50
0
MountPoints
#| Total size | Free | Type | Fsck / Cnt | W/D | State
00| 458 GiB | 155 GiB | raid1 | NO / 0 | W |
Harddisks
#|Disk |ID |Size |Type |Power |Smart |Temp |Parent
00|/dev/sda |WD-WMAYP5470669 |465 GiB |raid1 |ACTIVE/IDLE |NORMAL |41 |00
01|/dev/sdc |WD-WMAYP5506080 |465 GiB |raid1 |ACTIVE/IDLE |NORMAL |41 |00

24.6.1 Information

The following information is disclosed in the *Information* section:

Current write speed	The bitrate depends on video contents and may vary continuously. The average value is indicated in red.
Show target speed to record	By entering the required number of days in *Show target speed to record* and clicking **Set** you calculate the corresponding write speed. The red line will then be displaced to the obtained result. Recording behaviour will have to be modified to obtain the estimated bitrate.
Estimated days, base is current speed	Estimated hard disk storage capacity based on current measured bitrate. This value is expressed in number of days.
Estimated days, base is past recording	Estimated hard disk storage capacity based on existing footage stored on the hard disk. This value is expressed in number of days.
Free space for recording	This value is expressed in MB.

24.6.2 Mount Points

Because of the RAID 1 possibility the hard disks are not identical to the writing disks used by the RMG system. In the *MountPoints* section you get an overview of the writing disks that are in use.

24.6.3 Harddisks

In the **Harddisks** section you get a list of all hard disks that have been installed in the video system. For each hard disk you can see the free disk capacity and the total disk capacity. You will also see which disks have been put in RAID 1.

Appendix A: Abbreviations

3G: third generation

AGC: automatic gain control

APN: Access Point Name

A/V card: audio/video card

BNC: Bayonet Neill–Concelman

Cam: camera

CBR: constant bitrate compression

CD: compact disk

CIF: common intermediate format

CMS: central monitoring station

CPU: central processing unit

DEOL: dual end of line

/dev/ttyU1: USB input 1

DHCP: Dynamic Host Configuration Protocol

DIN: Deutsches Institut für Normung (German national organisation for standardisation)

DNS: domain name system

DTC: down the coax

DVD: digital video disk

EIO: Extension I/O

EMS: Event Management System

ETH: Ethernet interface

fps: frames per second

GB: gigabyte

GDI: Graphics Device Interface

GHz: gigahertz

GUI: graphical user interface

HD: high definition

HDD: hard disk drive

HTTP: hypertext transfer protocol

IC: interconnection

ID: identifier

I/O: input/output

IP: internet protocol

ips: images per second

ISDN: Integrated Services for Digital Network

IT: Information Technology

jpg: Joint Photographic Experts Group

kbps: kilobit per second

LAN: local area network

LED: light emitting diode

MAC: Media Access Control

MB: megabyte

MIC: microphone

MIO: Main I/O

NC: normally closed

NEOL: no end of line

NO: normally open

NTP: network time protocol

OSD: on screen display

OSID: Open-Area Smoke Imaging Detection

OTB: on the box / on the board

PAL: Phase Alternating Line

PC: personal computer

PIN: personal identification number

PIR: passive infrared

PoE: power over Ethernet

PPP: point-to-point protocol

PSTN: public switched telephone network

PTZ: pan tilt zoom

QCIF: quarter CIF

RAID: redundant array of independent disks

RMG: Remotely Managed Multiservice Gateway (= FastTrace 2 Series device)

RTSP: real-time streaming protocol

SDK: software development kit

SEOL: single end of line

SIF: source input format

SIM: subscriber identity module

SMART: Self-Monitoring, Analysis, and Reporting Technology

SMTP: Simple Mail Transfer Protocol

SP: Service Pack

SVGA: Super Video Graphics Array

Sync: synchronisation

TCP: transmission control protocol

Tx: transmission

UDP: user datagram protocol

USB: Universal Serial Bus

VBR: variable bitrate compression

VCP: VideoCentral Platinum

VDC: voltage direct current

VGA: Video Graphics Array

YUV: colour space with separate luminance (brightness) and chrominance (colour) components.

www.xtralis.com

UK and Europe +44 1442 242 330 **D-A-CH** +49 431 23284 1 **The Americas** +1 781 740 2223
Middle East +962 6 588 5622 **Asia** +86 21 5240 0077 **Australia and New Zealand** +61 3 9936 7000

A *Disclaimer* about this document, statements about *Intellectual Property, Copyrights*, and *Liability*, as well as a *General Warning* are available in an earlier section of this document.

Doc. 21796_05_preliminary

ADPRO® by xtralis®